アマゾン ウェブ サービス: リスクとコンプライアンス

2013 年 6 月

（本書の最新版については、http://aws.amazon.com/compliance 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 の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となっています。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は、AWS 固有の情報について掲載しています。

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お客様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。
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。

- 業界における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。
- NDA に従い（必要に応じて） 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。

責任共有環境

IT インフラストラクチャを AWS に移行すると、お客様と AWS の責任共有モデルが構成されます。この共有モデルでは、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。 これにより、 お客様の運用上の負担を支援し、軽減することが可能です。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、暗号化と鍵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も可能です。この責任共有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デプロイを可能となる柔軟性とお客様による統制ががもたらされることになります。

このお客様と AWS の責任共有モデルは IT 統制にも拡張され、適用されることになります。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、および検証についても分担となります。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することが可能になります。お客様によって AWS の適用形態は異なります。特定の IT 統制の管理を AWS に移行し、（新しい）拡張された統制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」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続きを実行できます。

次のセクションでは、AWS のお客様が拡張された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。

高水準のコンプライアンスとガバナンス

IT の適用形態にかかわらず、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ガバナンス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的と要件の把握、その目的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、統制環境の運用状況の検証などがあります。AWS クラウドのご利用にあたっては、様々な検証方法や各種統制の形態といった選択肢が存在します。

お客様の高水準なコンプライアンスとガバナンスの達成として、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とガバナンス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可能となります。また、実行すべき検証活動を明確化することも可能です。

AWS の統制の評価と統合

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支援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 環境における統制が効果的に機能しているかどうかを明確化し、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状況の検証は、社内外の監査人がプロセスを実地検証し、証跡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査または検証は、一般的に、その統制の妥当性を確認するために行われることになります。AWS などのサービスプロバイダを使用する場合、お客様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、統制の目標、統制の設計、運用状況に関する合理的な保証を得ることになります。その結果、お客様の主要な統制の項目の一部を AWS が管理している場合でも、お客様の統制環境を統一されたフレームワークとして維持し、その統制について把握し、運用状況について検証することが可能となります。AWS が取得している第三者からの証明と認証により、統制環境に対する高水準の検証を実施できるだけでなく、AWS クラウド上の IT 環境について、自身で特定の検証作業が必要となるお客様の要求の支援ともなります。

AWS の IT 統制情報

AWS は、次の 2 つの方法で IT 統制に関連する情報をお客様に提供します。

1. **特定の統制定義。** AWS のお客様は、AWS によって管理される重要な統制手続を特定することが可能です。重要な統制手続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、その重要な統制手続の運用状況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 統制に関する情報を公開しています。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） 」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になります。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） の設計と運用状況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、その妥当性に関して評価されるだけでなく、運用状況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 の外部監査人の独立性とその適正性により、レポートの記載事項は、AWS の統制環境の高い信頼性についての情報を、お客様にご提供するものとなっています。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、効果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了するために SOC 1 Type II レポートを要求する場合があります） 。

他の特定の統制活動は、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 が公開された基準に従っていることについて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 を特定の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も準拠しており、FISMA 基準にも準拠しています。このような一般的な基準に準拠しているため、お客様は特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することが可能です。

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、お客様のガバナンスフレームワークに AWS の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。これらの情報は、AWS が重要な一旦として組み込まれたガバナンスフレームワークと全体の統制を文書化することについて、お客様を支援する内容になっています。

リスク管理

AWS マネジメント層は、リスクの特定、また、リスクを緩和、管理するための統制の実装などを含む戦略的事業計画を作り上げています。 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、COBIT(the Control Objectives for information and related Technololgy) 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ています。また、ISO 27002 規格、米国公認会計士協会（AICPA）Trust サービスの原則、PCI DSS v2.0、 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管理策） に基づいて、ISO 27001 認証対応フレームワークを効果的に統合しています。。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施します。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となっています。

AWS セキュリティは、インターネットに接している全てのサービスエンドポイント IP アドレスに関して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されます。さらに、脆弱性に対する外部からの脅威のアセスメントが、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。これらのアセスメントに起因する発見や推奨事項は、分類整理された後に 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実行可能性を確認するためのものであり、お客様固有のコンプライアンス要件に適合する必要のある、お客様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。お客様は事前に承諾を得た上で、ご利用中のクラウドインフラストラクチャに対して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 適正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側面を活用し、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たものです。この包括的な統制環境は、AWS の統制の運用状況の有効性を支えるための環境を確立し、また、維持するために必要な、人員、プロセス、テクノロジーを網羅するものです。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ています。AWS は、お客様の統制環境の管理を支援するために、先進的な取り組みが実施されるアイデアを確認し、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、当社の最上層部を起点としています。役員とシニアリーダーは、当社の姿勢と本質的な価値感を確立する際に、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講しています。作成したポリシーを従業員が理解し、そのポリシーにしたが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、業務効率性、そして職務の分離がもたらされることになります。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ています。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装しています。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 は連邦政府による FedRAMP 適合クラウドサービスプロバイダです。AWS は、
FedRAMP の認可を受けた第三者評価機関（3PAO）が実施するテストに合格し、FedRAMP 要件に Moderate インパクトレベルで準拠していることが実証され、米国保健福祉省（HHS）から 2 つの Agency Authority to Operate （ATO）を付与され

ています。米国のすべての政府機関は、AWS の FedRAMP リポジトリに保存された Agency ATO パッケージを用いて、AWS がその機関のアプリケーションやワークロードに利用可能であるかの評価、AWS の使用認可の提供、
およびワークロードの AWS 環境への移行を行えます。2 つの FedRAMP Agency ATO は米国の全リージョン（AWS GovCloud（米国）リージョンと AWS 米国東部/西部リージョン）を包括しており、これらリージョンに対する認可範囲には以下のサービスが含まれます: Amazon Elastic Compute Cloud（EC2）、Amazon Simple Storage Service（S3）、Amazon Virtual Private Cloud（VPC）、Amazon Elastic Block Store（EBS）。AWS FedRAMP コンプライアンスの詳細については、AWS FedRAMP FAQ を参照してください。

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指定する米国政府のセキュリティ基準です。FIPS 140-2 の要件をお持ちのお客様をサポートするため、AWS GovCloud（米国）の Amazon Virtual Private Cloud VPN エンドポイントおよび SSL 終端 Load Balancer は、FIPS 140-2 検証済みのハードウェアを使用して運用しています。AWS は、AWS GovCloud（米国） 環境をご利用いただくときの、該当の要件に関するコンプライアンス管理に有益な情報をお客様に提供します。

FISMA と DIACAP

AWS では、米国政府機関のお客様がシステムについて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、その状態を維持することが可能です。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管理フレームワーク（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取得を達成しています。米国の政府機関は、AWS のセキュアなインフラストラクチャを利用することで、クラウドコンピューティングの活用の範囲を拡大させており、連邦政府の厳格なセキュリティ要件を満たし、政府の機密データやアプリケーションをクラウド環境に展開しています。

HIPAA

米国の医療保険に関する法律である The U.S. Health Insurance Portability and Accountability Act（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（Business Associate Agreements）を締結していく意向です。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、お客様が AWS を利用して、どのように HIPAA と別の医療に関する法律である Health Information Technology for Economic and Clinical Health （HITECH）コンプライアンスに準拠する必要のあるシステムについて処理を行うか、といった概要の説明になっています。

ISO 27001

AWS は自社の情報セキュリティマネジメントシステム（ISMS）に関する ISO 27001 認証を取得済みです。このシステムの範囲は AWS インフラストラクチャ、データセンター、および以下の各サービスに及びます: Amazon Elastic Compute Cloud（EC2）、Amazon Simple Storage Service（S3）、Amazon Virtual Private Cloud（VPC）、Amazon Elastic Block Store（EBS）、Amazon Relational Database Service（RDS）、Amazon DynamoDB、Amazon SimpleDB、Amazon Direct Connect、Amazon VM Import/Export、Amazon Glacier、Amazon Storage Gateway。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、会社と顧客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たものです。これは、刻々と変化する脅威のシナリオに適した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 のコミットメントを強化するものです。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しています。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ています。

ITAR

AWS GovCloud（米国）リージョンは、米国の国際武器取引規則（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、保護対象であるデータへのアクセスを米国人に限定し、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、意図しない輸出を統制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 人事によるアクセスを米国人に限定するという環境を提供しているため、適格企業は、ITAR の下で、保護対象の項目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、お客様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 で準拠しています。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 準拠の技術インフラストラクチャ上で、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 をリリースしました。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が記載されています。AWS では、お客様向けに PCI DSS Cloud Computing Guidelines を AWS PCI Compliance Package に組み込んで提供しています。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 2.0 下のレベル 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 とクラウドの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について説明がなされています。AWS PCI DSS レベル 1 認証には、SOC1 レポートの範囲とされているもの全てが含まれています。Amazon Elastic Compute Cloud（EC2）、Amazon Simple Storage Service（S3）、Amazon Virtual Private Cloud（VPC）、Amazon Elastic Block Store（EBS）、Amazon Relational Database Service（RDS）、Amazon DynamoDB、Amazon SimpleDB、Amazon Direct Connect、Amazon Glacier、Amazon Elastic MapReduce（EMR）、およびこれ

らを世界の全リージョンで稼働させているインフラストラクチャが対象です。AWS PCI DSS コンプライアンスの詳細については、PCI DSS Level 1 FAQ を参照してください。

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、保証業務基準書第 16 号（SSAE16）および国際保証業務基準書第 3402 号（ISAE 3402）の基準に従って実施されます。この 2 つの基準に沿ったレポートは、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成されています。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、およびお客様のデータを保護するために定義された個々の統制が有効に機能していることを証明するものです。この監査は、監査基準書第 70 号（SAS 70）Type II レポートに代わって行われているものです。

AWS SOC 1 の統制目標は以下のようなものとなっています。レポートには、各統制目標と独立監査人による手続に則った各項目に対するテストの結果を裏付ける内容として、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、合理的な保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、合理的な保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の処理の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 I T 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、お客様の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 の顧客層は広大で、AWS サービスの利用方法も同様に多種多様なため、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致するために、IT に関する幅広い一般的な統制を対象に設計されています。この事により、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の、重要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。

AWS の SOC 1 レポートへのコミットメントは継続的なものであり、これからも定期監査のプロセスを維持します。SOC 1 レポートの範囲には、Amazon Elastic Compute Cloud（EC2）、Amazon Simple Storage Service（S3）、Amazon Virtual Private Cloud（VPC）、Amazon Elastic Block Store（EBS）、Amazon Relational Database Service（RDS）、Amazon DynamoDB、Amazon SimpleDB、Amazon Direct Connect、Amazon VM Import/Export、Amazon ElastiCache、Amazon Glacier、Amazon Storage Gateway、Amazon Elastic MapReduce（EMR）、Amazon Redshift、AWS Identity and Access Management（IAM）、およびこれらを世界の全リージョンで稼働させているインフラストラクチャが含まれます。

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。統制の評価という点において SOC 1 と同様となりますが、SOC 2 レポートではその評価を、米国公認会計士協会（AICPA） の Trust サービス原則（Trust Services Principles）で定められている基準にまで拡張した内容の証明レポートとなっています。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な実践的統制が定義されています。AWS SOC 2 は、統制に関する設計上、および運用状況の有効性において、AICPA の Trust サービス原則基準によって定められているセキュリティ原則の基準を満たすものであるかどうかを評価した内容です。このレポートにより、主要な実践として事前定義されている業界標準に基づき、AWS のセキュリティに関してより一層の透明性がもたらされることになり、お客様のデータの保護に対する AWS のコミットメントが実証されることになります。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 レポートを一般公開用に要約したもので、AICPA SysTrust セキュリティシールを掲示することができます。レポートには、統制の運用に対する外部監査人の（SOC 2 レポートに含まれる AICPA の Security Trust Principles に基づく）意見、統制の有効性に関する AWS 経営本部からのアサーション、AWS インフラストラクチャと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有益な資料です。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イニシアチブ

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）」に対して回答済みです。CSA が発行するこの調査フォームは、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 1 つの手段となっています。
  CAIQ は、クラウドの利用者やクラウド監査担当者の視点からクラウドプロバイダーに尋ねる、140 項目を超える質問で構成されています。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:*** 米国映画協会（MPAA）は、保護対象のメディアやコンテンツを安全に保存、処理、および配信するための一連のベストプラクティス（http://www.fightfilmtheft.org/facility-security-program.html） を確立しています。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ための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適用可能なすべての 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、AWS の回答を掲載しています。このような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際に関係するものや、AWS のお客様が統制を管理していく際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 内にデプロイされている部分については、AWS がそのテクノロジーに関するの物理コンポーネントを統制します。その他の部分は、接続ポイントやデータ送信の統制を含め、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、それがどのように有効的に運用されているかに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に関する統制を公表しています。これらの統制はハイレベルで定義されているため、ほとんどのお客様の要件を満たすことになります。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可能です。
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 によって定義された論理統制と物理統制の記述は、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可能となっています。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可能です。
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 クラウド上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することになります。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。ほとんどの論理的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するかどうかは、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 によって提供され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 のお客様が統制することになります。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、あるいはそれ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は、すでにお客様によって AWS 上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。
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 のお客様によって統制されることになります。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有効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?	米国の連邦機関が準拠できる規格には、2002 年の連邦情報セキュリティマネジメント法（FISMA）、連邦政府によるリスクと認証管理プログラム（FedRAMP）、連邦情報処理規格（FIPS）出版物 140-2、米国国際武器取引規則（ITAR）などがあります。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と考えられます。
7	データの場所。ユーザーデータはどこにありますか?	データとサーバを配置する物理的なリージョンは、AWS のお客様が指定することになります。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内のクラスタで実行され、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 のお客様が指定することになります。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。
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 のデータセンターでは複数のお客様をホストしており、幅広いお客様を第三者の物理的アクセスにさらすことになるという理由から、お客様によるデータセンター訪問を許可していません。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存在と運用について検証を行っています。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、お客様は実施されている統制の有効性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セキュリティの独立した見直しは、ISO 27001 監査、PCI 評価、ITAR 監査、および FISMA テストプログラムにも含まれています。
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。AWS の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が明示的に承認した場合を除き、サードパーティには AWS データセンターへのアクセスは付与されません。物理アクセス、データセンターアクセスの許可などの関連する具体的な統制については、SOC 1 Type II レポートをご覧ください。
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限定し、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。特権的ユーザアクセス統制は、AWS SOC 1、ISO 27001、PCI、ITAR、および FedRAMP の監査時の独立監査人による審査対象となっています。
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に SOC 1 統制を規定しています。また、本文書で解説されている公開認定およびコンプライアンスの取り組みでは、内部者へのアクセスの対処について言及されています。すべての認定とサードパーティによる証明は、予防的、見地的な側面から論理アクセスに関する統制を評価するものです。さらに、定期的なリスク評価では、内部者によるアクセスがどのように統制され。監視されるかといった点について重点的に取り組んでいます。

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ています。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、独立した PCI Qualified Security Assessor（QSA）による検証を受け、2010 年 10 月に発行された PCI DSS バージョン 2.0 のすべての要件に準拠しているという結果が出ています。 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 クラウドの利点を最大限に活用しながら、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入対策チームが新規および既存の脆弱性とアタックベクター（Attack Vectors）を定期的に評価しており、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合するものです。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も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についての詳細については、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。これらの作業は AWS のポリシーによって必要とされるものですが、同時に ISO 27001、NIST、および PCI の要件に準拠して、必要に応じて実行されるものです。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つことになります。

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 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ーを使用することも可能です。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。
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。
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、強力なテナントの隔離のためのセキュリティと統制機能によって保護されています。Amazon S3 は高度なデータアクセス統制を提供しています。具体的なそれぞれのデータサービスに関する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、AWS がサポートする他の認定（ISO 27001、FISMA など）においても、物理および環境に関する統制のベストプラクティスが必要となっています。
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 では一連の アイデンティティとアクセス管理に対するサービス（AWS IAM）を提供しています。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可能です。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 クラウドは分散型で、高いセキュリティと回復力をもったサービスのため、大規模な拡張が可能となる潜在能力を持っています。お客様は、システムをスケールアップ、あるいはスケールダウンすることが可能で、使用したサービス内容に対する料金のみをお支払いいただくだけとなっています。
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。
27	分散サービス妨害（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 のネットワーク環境においては、従来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することも可能です。
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、堅牢なビジネス継続性に関する設計を実装するための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冗長的に保存されます。オブジェクトが格納された後は、Amazon S3 は冗長性が失われた場合には、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 99.99% 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が可能です。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と将来性があります。

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 のセキュリティに関する詳細については、AWS セキュリティセンターや AWS セキュリティプロセスの概要ホワイトペーパー を参照してください。メールでのお問い合わせは aws-security@amazon.com にて承ります。

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における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利用を促進し、クラウドコンピューティングの使用に関する教育を提供することで、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った非営利組織」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、クラウドの利用者およびクラウドに係る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 はこの調査票に対する全ての回答を完成させています。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、各種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、それらの認定、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、外部からの脆弱性脅威アセスメントが、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。これらのアセスメントに起因する発見や推奨事項は、分類整理され、AWS 上層部に報告されます。 さらに、AWS の統制環境は、定期的な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 の統制環境全体に対して確認、およびテストを実施しています。
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?	

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	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 のセキュリティチームは、独立したセキュリティ会社と契約し、定期的に外部の脆弱性脅威アセスメントを実施しています。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		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?	
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関係を維持しています。
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。お客様のデータの所有権はお客様が保持します。したがってデータの暗号化を選択するのはお客様の責任となります。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 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。
		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は、Control Objectives for Information and related Technology (COBIT) Framework に基づき、情報セキュリティのフレームワークとポリシーを確立しています。また、AWS のセキュリティフレームワークには、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が統合されています。 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。

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-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。
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保持します。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 サービスの一環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。メタデータの一つの形式である 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。お客様はさらに条件を追加して、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に、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、9 つのリージョンが存在します。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
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?	

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
				パウロ）です。
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保持します。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。
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保持していますので、お客様の要件に応じてデータの保持期間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

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-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。	ています。AWS は、DoD 5220.22-M（「National Industrial Security Program Operating Manual（国立産業セキュリティプログラム作業マニュアル）」）または NIST 800-88（「Guidelines for Media Sanitization（メディア衛生のためのガイドライン）」）に詳細が記載されている技術を用いて、廃棄プロセスの一環としてデータを破棄します。これらの手順を用いて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	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保持しています。AWS では、お客様自身で運用環境および非運用環境を保守および開発することが可能です。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装しています。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、物理的なホストや、お客様自身に割り当てられていないインスタンスにアクセス不可能な設計となっています。このアーキテクチャは、独立した PCI Qualified Security Assessor（QSA）による検証を受け、2011 年 6 月に発行された PCI DSS バージョン 2.0 のすべての要件に準拠しているという結果が出ています。 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		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?	
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。関連する認定やレポートを AWS のお客様に提供することが可能です。 継続的な倫理的統制のモニタリングについては、お客様が自身のシステム上で実施可能です。

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
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内において、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に関する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。また、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	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、9 つのリージョンが存在します。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 ウェブサイト （http://aws.amazon.com for additional details）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	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。
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 （「National Industrial Security Program Operating Manual（国立産業セキュリティプログラム作業マニュアル）」）または NIST 800-88 （「Guidelines for Media Sanitization（メディア衛生のためのガイドライン）」)に詳細が記載されている技術を用いて、廃棄プロセスの一環としてデータを破棄します。これらの手順を用いて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 専有の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

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		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?	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。
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、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。 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、修了時に受講確認が必須となる定期的な情報セキュリティトレーニングを受けています。作成したポリシーを従業員が理解し、そのポリシーに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。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?	
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契約終了、役職の変更に伴う社内の管理責任について規定しています。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）、総務、および各サービスオーナー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 プログラムについて知る必要のあるお客様に、ISO 27001 認定文書を提供しています。

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
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 フレームワークによって、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、当社の最上層部を起点としています。役員とシニアリーダーは、当社の姿勢と本質的な価値観を確立する際、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?	
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。

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		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?	

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	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、修了時に受講確認が必須となる定期的な情報セキュリティトレーニングを受けています。作成したポリシーを従業員が理解し、そのポリシーに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。
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?	

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	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	経営層は、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、当社の最上層部を起点としています。役員とシニアリーダーは、当社の姿勢と本質的な価値観を確立する際、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講しています。作成したポリシーを従業員が理解し、そのポリシーに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、お客様の AWS 上のリソースについて、役割分担を管理することが可能です。 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、様々な手段の内部コミュニケーションをグローバルレベルで実施し、従業員が各自の役割と職責を理解するために支援をし、重要なイベントを時宜にかなった方法で通知しています。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。詳細については、ISO 27001 規格
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?	

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-16.3	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?	の附属書 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	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。詳細については、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活動について、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 のサーバーサイド暗号化サービスを利用しない場合、お客様独自の暗号化メカニズムについて管理することになります。サーバーサイド暗号化サービスの場合、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 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サイド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 鍵管理手続きは、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 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-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	鍵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	シグネチャー、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	インシデント管理	IS-22.1	文書化したセキュリティインシデント対応計画がありますか?	AWS のインシデント対応プログラム、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 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。
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インシデント対応計画に統合していますか?	

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		IS-22.3	セキュリティインシデント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?	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	インシデントのレポート	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、物理アクセスログなど）を結合していますか?	AWS のインシデント対応プログラム、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インシデントを分離できますか?	
情報セキュリティ	インシデント対応の法的準備	IS-24.1	インシデント対応計画は、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 のインシデント対応プログラム、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。お客様の代理で AWS が保存しているすべてのデータは、強力なテナントの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	インシデント対応機能には、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	インシデント対応のメトリクス	IS-25.1	すべての情報セキュリティインシデントの種類、規模、および影響を監視および数値化していますか?	AWS のセキュリティメトリクスは、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。

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-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?	
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、お客様の環境におけるプライバシー違反について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 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サイド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 リソースへの論理的なアクセスに関する基準を規定するための、公式のポリシーと手続きを確立しています。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。

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	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?	管理レベルにアクセスする必要のある作業を担当する管理者は、Multi-Factor Authentication 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、クラウドの管理レベル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。管理レベル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?	
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 リソースへの論理的なアクセスに関する基準を規定するための、公式のポリシーと手続きを確立しています。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 リソースへの論理的なアクセスに関する基準を規定するための、公式のポリシーと手続きを確立しています。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?	

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	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され監視されています。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?	
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通じ、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コミットメントをお客様に知っていただくために、各種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?	

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	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取得し復元が可能です。お客様は、AMI （Amazon Machine Image）をエクスポートして、お客様の恩プレミス環境または別のプロバイダにおいて使用できます （ただし、ソフトウェアのライセンス制限事項に従うことになります）。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、お客様に賠償を提供しています。
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?	
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）?	

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	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 Risk and Compliance Whitepaper」（http://aws.amazon.com/security）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、自動プロセスにより、お客様のデータトラフィックを影響下にあるエリアから移動させます。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。詳細については、ISO 27001 基準の付録 A、ドメイン 11.2 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。
		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?	
		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。

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	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 レポートでは、AWS 環境における変更管理についての管理体制に関する概要に関しての情報を提供しています。 また、詳細については、ISO 27001 基準の付録 A、ドメイン 12.5 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?	
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。

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	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 のクラウドリソースと AWS 上でお客様が実行するアプリケーションについてのモニタリング機能を提供します。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。お客様は、複数のリージョンやアベイラビリティゾーンを活用可能な利点を考慮し、AWS の利用について設計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 の事業継続計画（BCP, Business Continuity Plan）は、ISO 27001 基準に合わせて開発され、テストされています。 AWS と事業継続性（Business Continuity）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	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 および AWS SOC 1 Type II 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	設備の場所	RS-06.1	影響が大きい環境リスク（洪水、竜巻、地震、ハリケーンなど）の可能性/発現度が高い場所にあるデータセンターはありますか?	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。お客様は、複数のリージョンやアベイラビリティゾーンを活用可能な利点を考慮し、AWS の利用について設計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、適用可能となる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 Trusted Cloud Architectural Standard、FedRAMP CAESARS）	AWS Data Security Architecture は、業界の最先端の実践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）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 のデータ整合性に関する統制は 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保持します。AWS 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?	

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	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。
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 ウェブサイトは、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において、レイヤードセキュリティアーキテクチャ（Layered Security Architecture）作成に関する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、お客様が定義する要件に従って、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配備されています。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?	

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	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対して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 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	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、およびインシデント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 インシデント対応プログラム（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。

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		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: 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

米国映画協会（MPAA）は、保護対象のメディアやコンテンツを安全に保存、処理、および配信するための一連のベストプラクティス（http://www.fightfilmtheft.org/facility-security-program.html）を確立しています。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評価とセキュリティ監査の手段として使用しています。

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、下記を参照してください。

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
エグゼクティブによるセキュリティの認識/監督	MS-1.0	情報セキュリティプログラムとリスクアセスメント結果の定期的な見直しを義務付けることにより、経営陣やオーナーが情報セキュリティ機能を確実に監督するようにします。	Amazon の統制環境は、当社の最上層部を起点としています。役員とシニアリーダーは、当社の姿勢と本質的な価値感を確立する際、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の完了が必要となります。規定されたポリシーの理解と遵守を従業員に徹底するために、コンプライアンス監査を実施します。 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。
エグゼクティブによるセキュリティの認識/監督	MS-1.1	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。	
リスク管理	MS-2.0	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重要資産に焦点をあてた正規のセキュリティリスクアセスメントプロセスを作成します。	お客様は自らのデータの所有権を保持し、そのデータのワークフローに関連するリスクの査定と管理について各自のコンプライアンス要件を満たす責任を負います。 AWS は顧客情報および関連する資産をすべて極秘として扱います。AWS は、ISO 27001 に基づき、リスク管理プログラムを作成してリスクの軽減と管理に努めています。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。 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 が実施する個別の統制活動については AWS SOC 1 Type II レポートと AWS SOC 2 Type II レポートに詳しく記載されています。
リスク管理	MS-2.1	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。	
リスク管理	MS-2.2	セキュリティリスクアセスメントを毎年実施し、主要ワークフローが変化する際にリスクアセスメントを見直し、特定されたリスクについては文書化し対策を実施します。	
セキュリティ組織	MS-3.0	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。 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。また、AWS SOC 1 Type II レポートおよび AWS SOC 2 Type II レポートにも 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。

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
予算編成	MS-4.0	セキュリティの構想、向上、維持を文書化し、予算に計上します。	AWS の情報セキュリティとコンプライアンスに関連する組織は、行動計画やスケジュールを作成し、セキュリティ構想を明確にして、AWS 情報セキュリティプログラムの強化を図る役割を担います。AWS CISO は、行動計画、日程表、予算などの決裁を行い、AWS がセキュリティに関する取り組みの強化に継続的に努めるようサポートする役割を担います。 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。
ポリシーと手順	MS-5.0	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 • 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	お客様のデータに関する責任、およびコンテンツのセキュリティを管理するための関連ポリシーと手順を作成する責任は、お客様にあります。 AWS の情報資産にかかわるポリシーおよび手順は、AWS Information Security により、COBIT フレームワーク、ISO 27001 規格、および PCI DSS 要件に基づいて制定されています。ISO 27001 基準に合わせて、すべての AWS 従業員は、修了時に受講確認が必須となる定期的な情報セキュリティトレーニングを受けています。作成したポリシーを従業員が理解し、そのポリシーに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。 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 レポートおよび AWS SOC 2 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 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
ポリシーと手順	MS-5.1	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。	
ポリシーと手順	MS-5.2	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。	
インシデント対応	MS-6.0	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。	お客様の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に関する統制はお客様が保持し、お客様の組織の要件を満たすインシデント対応プランの作成はお客様の責任となります。 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。
インシデント対応	MS-6.1	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。	

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
インシデント対応	MS-6.2	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。	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。
インシデント対応	MS-6.3	漏えい、盗難、またはその他の形で欠損したコンテンツ（例: 紛失した顧客の資産）の所有者である顧客に、インシデント発生について速やかに連絡し、経営陣と顧客を交えて事後対策会議を開きます。	
ワークフロー	MS-7.0	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	お客様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、およびデータに関する統制はお客様が保持し、お客様のリスクおよびコンプライアンス要件を満たすコンテンツワークフローの文書化はお客様の責任となります。 ISO 27001 基準に合わせ、AWS のハードウェア資産を所有者に割り当て、追跡、監視する作業は、AWS の担当者が AWS の独自開発したインベントリ管理ツールで行います。 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。
ワークフロー	MS-7.1	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。	
役割分担	MS-8.0	コンテンツのワークフロー内で役割を分担します。	お客様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、およびデータに関する統制はお客様が保持し、お客様の環境における役割分担の実施はお客様の責任となります。 AWS は ISO 27001 基準に合わせて役割の分担を行います。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。
役割分担	MS-8.1	役割の分担が現実的でない部分について、補足コントロールを実装・文書化します。	
経歴確認	MS-9.0	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。 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。

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
守秘契約	MS-10.0	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。 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。
守秘契約	MS-10.1	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。	
懲戒処分	MS-11.0	施設ポリシー違反に対する懲戒処分を定め、従業員とサードパーティの従業員の全員に周知させます。	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を行っています。Amazon の基準または手続きに違反した従業員は調査され、適切な懲戒的措置（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。
コンテンツセキュリティと著作権侵害への啓発	MS-12.0	セキュリティ啓発プログラムを作成して定期的に更新すると同時に、従業員およびサードパーティの従業員に採用時とその後年 1 回の研修を行います。研修には最低限以下の内容を含むものとします。 • 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	ISO 27001 基準に合わせて、すべての AWS 従業員は、修了時に受講確認が必須となる定期的な情報セキュリティトレーニングを受けています。作成したポリシーを従業員が理解し、そのポリシーに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。 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 レポートおよび AWS SOC 2 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 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。
サードパーティの利用と審査	MS-13.0	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。	お客様の製品範囲およびデータに関する統制はお客様にあり、お客様のリスクおよびコンプライアンス要件を満たすサードパーティポリシーの作成はお客様の責任となります。 Amazon 機密保持契約書（NDA）は Amazon Legal Counsel が管理し AWS の業務要件を反映させています。機密保持契約書は AWS が使用するサードパーティの請負業者、販売業者、および従業員に交付されます。 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。
サードパーティの利用と審査	MS-13.1	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。	
サードパーティの利用と審査	MS-13.2	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。	
サードパーティの利用と審査	MS-13.3	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。	

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
サードパーティの利用と審査	MS-13.4	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。	
サードパーティの利用と審査	MS-13.5	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。	
出入り口	PS-1.0	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。	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。データセンターのフロアにアクセスするには、権限を与えられたスタッフが 2 要素認証を最低 2 回パス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。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。
出入り口	PS-1.1	コンテンツ/制作エリアを施設の他のエリア（管理事務所など）から分離することによって、制作エリアへのアクセスを制限します。	
出入り口	PS-1.2	アクセス制限エリア（映写ブースなど）への立ち入りに際しスクリーニングを行うための部屋を設けます。	
訪問者の出入り	PS-2.0	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 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された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。 AWS SOC 1 Type II レポートおよび AWS SOC 2 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 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
訪問者の出入り	PS-2.1	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。	
訪問者の出入り	PS-2.2	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。	
訪問者の出入り	PS-2.3	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。	
身分証明書	PS-3.0	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承認された従業員に対し、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 SOC 1 Type II レポートおよび AWS SOC 2 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 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

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
周辺のセキュリティ	PS-4.0	組織のリスクアセスメントにより、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。	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。 AWS SOC 1 Type II レポートおよび AWS SOC 2 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 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
緊急時プロトコル	PS-5.0	緊急時、事故時、または停電時に、セキュリティ設備（例: 監視カメラシステム、警報システム、電子アクセスシステム）および重要な制作機器を少なくとも 15 分間維持して施設のセキュリティを確保する時間を稼ぐために、無停電電源（UPS）などの予備発電装置を設置します。	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 レポートおよび AWS SOC 2 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、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） も参照してください。
緊急時プロトコル	PS-5.1	少なくとも年に 1 度、予備発電装置のテストと保守を行います。	
緊急時プロトコル	PS-5.2	電子アクセスシステムを施設に設置する際には、停電時に備えてフェイルセキュアな構成にします。	
警報	PS-6.0	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/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。	物理的セキュリティ統制には、保安要員、監視カメラ、侵入検知システムが含まれます。警報が発生した場合には監視についている AWS の物理保安要員が対応します。データセンターのフロアにアクセスするには、権限を与えられたスタッフが 2 要素認証を最低 2 回パスする必要があります。 AWS SOC 1 Type II レポートおよび AWS SOC 2 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 リスクとコンプライアンスホワイトペーパーおよび 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
警報	PS-6.1	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。	
警報	PS-6.2	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。	
警報	PS-6.3	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。	
警報	PS-6.4	警報システムを 6 か月に 1 度テストします。	
警報	PS-6.5	制限エリア（例: 保管庫、サーバ/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。	

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
警報	PS-6.6	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。	
承認	PS-7.0	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。	AWS では、AWS データセンターに物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。カード所有者のデータセンターに対するアクセス権は、四半期ごとに見直されます。四半期ごとの見直しの一環で削除対象としてマークされたカード所有者は、アクセス権が取り消されます。 AWS SOC 1 Type II レポートおよび AWS SOC 2 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 リスクとコンプライアンスホワイトペーパーおよび 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
承認	PS-7.1	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/マシンルーム）へのアクセスを確認します。	
電子アクセス	PS-8.0	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。	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。 AWS SOC 1 Type II レポートおよび AWS SOC 2 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 リスクとコンプライアンスホワイトペーパーおよび 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
電子アクセス	PS-8.1	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。	
電子アクセス	PS-8.2	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。	
電子アクセス	PS-8.3	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。	
電子アクセス	PS-8.4	電子アクセスシステムを設置した制限エリア（例: 保管庫、サーバ/マシンルーム）から物理的な施錠装置を撤去します。	
電子アクセス	PS-8.5	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。	
キー	PS-9.0	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 SOC 1 Type II レポートおよび AWS SOC 2 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 リスクとコンプライアンスホワイトペーパーおよび 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
キー	PS-9.1	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。	
キー	PS-9.2	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。	
キー	PS-9.3	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。	

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
カメラ	PS-10.0	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、CCTV（Closed Circuit Television Camera）を使用して録画されています。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 SOC 1 Type II レポートおよび AWS SOC 2 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 リスクとコンプライアンスホワイトペーパーおよび 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。
カメラ	PS-10.1	どのような照明条件下でもカメラの録画映像が明瞭に視認できるものとなるように調整を行います。	
カメラ	PS-10.2	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。	
カメラ	PS-10.3	カメラの位置、画質、フレームレート、および監視映像の適切な保持期間を週に 1 度確認します。	
カメラ	PS-10.4	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。	
ロギングとモニタリング	PS-11.0	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。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、CCTV（Closed Circuit Television Camera）を使用して録画されています。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 SOC 1 Type II レポートおよび AWS SOC 2 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 リスクとコンプライアンスホワイトペーパーおよび 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
ロギングとモニタリング	PS-11.1	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。	
ロギングとモニタリング	PS-11.2	すべての確認済みの電子アクセスインシデント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。	
ロギングとモニタリング	PS-11.3	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。	
検査	PS-12.0	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 は問題が生じた際に手荷物検査を実施する権利を有しています。
在庫トラッキング	PS-13.0	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。	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するのはお客様の責任となります。 ISO 27001 基準に合わせ、AWS のハードウェア資産を所有者に割り当て、追跡、監視する作業は、AWS の担当者が AWS の独自開発したインベントリ管理ツールで行います。 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
在庫トラッキング	PS-13.1	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。	
在庫トラッキング	PS-13.2	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。	

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
在庫トラッキング	PS-13.3	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。	査人から、検証および認定を受けています。
在庫トラッキング	PS-13.4	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。	
棚卸し	PS-14.0	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。 社内では、ISO 27001 基準に合わせ、AWS ハードウェア資産を所有者に割り当て、追跡、監視する作業は、AWS の担当者が AWS の独自開発したインベントリ管理ツールで行います。 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。
棚卸し	PS-14.1	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。	
棚卸し	PS-14.2	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。	
ブランクメディア/生フィルムのトラッキング	PS-15.0	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。メディア在庫のセキュリティを管理するのはお客様の責任となります。
ブランクメディア/生フィルムのトラッキング	PS-15.1	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。	
顧客の資産	PS-16.0	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。	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へのアクセスを制限するのはお客様の責任となります。 社内では、ISO 27001 基準に合わせ、AWS ハードウェア資産を所有者に割り当て、追跡、監視する作業は、AWS の担当者が AWS の独自開発したインベントリ管理ツールで行います。 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。
顧客の資産	PS-16.1	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。	

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
制作システム	PS-17.0	制作システムへのアクセスを、適切な担当者のみに制限します。	お客様の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に関する統制はお客様にあり、お客様の本番環境に適切な制限を実装するのはお客様の責任となります。 AWS では、管理レベルにアクセスする必要のある作業を担当する管理者は、Multi-Factor Authentication 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、クラウドの管理レベル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。管理レベル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。 AWS SOC 1 Type II レポートおよび AWS SOC 2 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 リスクとコンプライアンスホワイトペーパーおよび 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
廃棄	PS-18.0	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。	お客様各自の要件に合わせて物理的メディア資産を廃棄する責任はお客様にあります。 AWS では、自社のストレージデバイスが耐用年数の終わりに達した際の廃棄プロセスとして、お客様のデータがアクセス権限を持たない人々に漏洩するのを防ぐ措置をとることが AWS 手順書により定められています。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。
廃棄	PS-18.1	米国国防総省（DoD）の定める消去とサニタイズの標準手順に従い、デジタルシュレッディングおよびワイピングを実施します。	
廃棄	PS-18.2	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。	
廃棄	PS-18.3	資産の廃棄記録は少なくとも 12 か月間保管します。	
廃棄	PS-18.4	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。	
廃棄	PS-18.5	確認用ディスクは使用後ただちに破棄します。	

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
出荷	PS-19.0	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。	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の出荷/搬入を管理するのはお客様の責任となります。 ISO 27001 基準に合わせ、AWS のハードウェア資産を所有者に割り当て、追跡、監視する作業は、AWS の担当者が AWS の独自開発したインベントリ管理ツールで行います。 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。
出荷	PS-19.1	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	
出荷	PS-19.2	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。	
出荷	PS-19.3	集荷待ちの資産のセキュリティを確保します。	
出荷	PS-19.4	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。	
入荷	PS-20.0	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。	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の出荷/搬入を管理するのはお客様の責任となります。 社内では、ISO 27001 基準に合わせ、AWS ハードウェア資産を所有者に割り当て、追跡、監視する作業は、AWS の担当者が AWS の独自開発したインベントリ管理ツールで行います。 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。
入荷	PS-20.1	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。	
入荷	PS-20.2	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	
入荷	PS-20.3	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。	
ラベル貼り	PS-21.0	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。	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の出荷/搬入手順を管理するのはお客様の責任となります。 ISO 27001 基準に合わせ、AWS のハードウェア資産を所有者に割り当て、追跡、監視する作業は、AWS の担当者が AWS の独自開発したインベントリ管理ツールで行います。
ラベル貼り	PS-21.1	出荷梱包にはすべて、クライアント名や企業名のほか、差出人住所を記載します。	

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
			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。
梱包	PS-22.0	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。	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の出荷/搬入を管理するのはお客様の責任となります。 ISO 27001 基準に合わせ、AWS のハードウェア資産を所有者に割り当て、追跡、監視する作業は、AWS の担当者が AWS の独自開発したインベントリ管理ツールで行います。 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。
梱包	PS-22.1	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）	
輸送車両	PS-23.0	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。	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の出荷/搬入を管理するのはお客様の責任となります。 社内では、ISO 27001 基準に合わせ、AWS ハードウェア資産を所有者に割り当て、追跡、監視する作業は、AWS の担当者が AWS の独自開発したインベントリ管理ツールで行います。 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。
WAN	DS-1.0	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。	Amazon EC2 は、完全なファイアウォールソリューションを提供します。この強制インバウンドファイアウォールは、デフォルトで deny-all モードに設定されており、Amazon EC2 のお客様が必要なポートを明示的に開かない限り、インバウンドトラフィックを受け入れることはありません。トラフィックは、プロトコルやサービスポートの他に、ソース IP アドレス （個別 IP またはクラスレスドメイン間ルーティング（CIDR）ブロック） でも制限することができます。Amazon RDS データベースインスタンスへのアクセスは、データベースセキュリティグループを介してお客様が制御できます。データベースセキュリティグループは Amazon EC2 セキュリティグループに似ていますが別途設定が必要となります。データベースセキュリティグループはデフォルトでは「deny all」アクセスモードになっており、ネットワークへのインバウンドアクセスはお客様が明示的に許可する必要があります。Amazon ElastiCache では、お客様がキャッシュセキュリティグループを使用して、キャッシュクラスターへのアクセスをコントロールすることができます。キャッシュセキュリティグループは、キャッシュクラスターへのネットワークアクセスをコントロールするファイアウォールのように動作します。AWS のお客様は、各自に定められた要件に合わせてファイアウォール設
WAN	DS-1.1	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。	
WAN	DS-1.2	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。	
WAN	DS-1.3	外部からアクセス可能なサーバ （例: セキュア FTP サーバ、ウェブサーバ） を DMZ 内に配置します。	
WAN	DS-1.4	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	

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
		期的に実施します。	定とネットワークセグメンテーションを管理する責任を有します。 AWS 社内では、ネットワークセグメンテーションは ISO 27001 規格に準拠しています。また、ファイアウォールデバイスが、Amazon の企業および実稼動ネットワークに対するアクセスを制限するよう設定されています。これらのファイアウォールポリシーの構成は、マスターサーバーからの 24 時間ごとの自動プッシュによって維持されています。 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。
WAN	DS-1.5	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。	
WAN	DS-1.6	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。	
WAN	DS-1.7	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に確保します。	
WAN	DS-1.8	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。	
WAN	DS-1.9	通信サービスプロバイダを介してファイバー接続を開設した場合は、セッション終了後に必ず接続を切断します。	
WAN	DS-1.10	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。	
インターネット	DS-2.0	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）へのインターネットアクセスを禁じます。	AWS のお客様の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、デスクトップ、メール、およびウェブフィルタリングに関する統制と所有権はお客様にあります。 メールフィルタリング、ウイルス対策、およびマルウェア対策ソフトウェアの管理に対する AWS のプログラム、プロセス、および手続きは、ISO 27001 規格に準拠しています。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。
インターネット	DS-2.1	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、コンテンツ/制作にかかわらないネットワークから、以下のものを遮断します。 • 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	
インターネット	DS-2.2	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。	

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
LAN	DS-3.0	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、物理的ないし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 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。
LAN	DS-3.1	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。	
LAN	DS-3.2	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。	
LAN	DS-3.3	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。	
LAN	DS-3.4	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。	
LAN	DS-3.5	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。	
LAN	DS-3.6	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。	
ワイヤレス	DS-4.0	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。	お客様のワイヤレスセキュリティを管理、監視、設定する責任はお客様にあります。

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
ワイヤレス	DS-4.1	制作/コンテンツにかかわらないネットワークにおけるワイヤレスネットワークに、強力なセキュリティ統制を組み込みます。 • SSID ブロードキャスティングを無効化 • WEP を無効化 • AES 暗号化を有効化 • IEEE 802.1X または IEEE 802.11i が利用可能であれば有効化 • 可能なら認証に RADIUS を使用 事前共有キーの使用が必要な場合は、以下の統制を導入します。 • WPA2 の暗号化方式として CCMP（AES）を指定 • 複雑なパスフレーズを設定 （パスフレーズを複雑化するための推奨手法については DS-8.1 を参照してください） • パスフレーズは定期的に変更し、主要な従業員が退職した場合にも随時変更する • MAC アドレスフィルタリングを有効化	Amazon のネットワーク環境とワイヤレスセキュリティを保護するためのポリシー、手順、メカニズムが配備されています。詳細については AWS SOC 1 Type II レポートおよび SOC 2 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。
ワイヤレス	DS-4.2	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。	
ワイヤレス	DS-4.3	対象エリアを限定してワイヤレスネットワーク接続を提供するためのワイヤレスアクセスポイントについては電波送信出力を下げます。	
I/O デバイスセキュリティ	DS-5.0	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。	お客様のデータの統制と所有権はお客様が保持します。したがってデータ暗号化の選択とデバイスへの入出力管理ポリシーの実装はお客様の責任となります。 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 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 鍵管理手続きは、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。
I/O デバイスセキュリティ	DS-5.1	入出力（I/O）デバイス（例: USB、Fire Wire、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。	
I/O デバイスセキュリティ	DS-5.2	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。	
I/O デバイスセキュリティ	DS-5.3	コンテンツ移送のために利用するハードドライブおよび USB フラッシュメモリには AES 128 ビット暗号化を施します。	

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
I/O デバイスセキュリティ	DS-5.4	機密コンテンツに電子的にアクセスできるエリアでは、デジタル記録デバイス（スマートフォン、デジタルカメラ、ビデオカメラなど）の使用を禁じます。	
システムセキュリティ	DS-6.0	すべてのワークステーションとサーバにアンチウイルスソフトウェアをインストールします。	お客様のコンテンツの開発、内容、運用、保守、および使用については、お客様が責任を負うものとします。お客様の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に関する統制はお客様にあり、お客様の環境の管理と運用に関するポリシー、手順、およびガイドラインの作成はお客様の責任となります。お客様はまた、自身のシステムに対する脆弱性スキャンの実施とパッチの適用について責任を負います。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。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。 ウイルス/マルウェア対策ソフトウェアの管理に対する AWS 社内のプログラム、プロセス、および手続きは、ISO 27001 規格に準拠しています。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。
システムセキュリティ	DS-6.1	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。	
システムセキュリティ	DS-6.2	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。	
システムセキュリティ	DS-6.3	ウイルススキャンの要領を文書化し実施します。以下はその例です。 • 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。	
システムセキュリティ	DS-6.4	定期的にセキュリティ脆弱性を修正する更新パッチを（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などに）適用するパッチ管理プロセスを実施します。	
システムセキュリティ	DS-6.5	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。	
システムセキュリティ	DS-6.6	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。	
システムセキュリティ	DS-6.7	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。	
システムセキュリティ	DS-6.8	ソフトウェアをインストールする権限はシステム管理者のみに制限します。	
システムセキュリティ	DS-6.9	あらゆるソフトウェアなどの専有ソフトウェア資産について正規ライセンスを使用することを義務付けます。	

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
システムセキュリティ	DS-6.10	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。	
システムセキュリティ	DS-6.11	コンテンツ転送サーバ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。	
アカウント管理	DS-7.0	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、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。	お客様の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に関する統制はお客様にあり、適切なアカウント管理手順の実装はお客様の責任となります。 AWS 社内では、ISO 27001 規格に基づき、AWS リソースへの論理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。管理レベルにアクセスする必要のある作業を担当する管理者は、Multi-Factor Authentication 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、クラウドの管理レベル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。管理レベル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は取り消されます。 AWS SOC 1 Type II レポートおよび SOC 2 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 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。
アカウント管理	DS-7.1	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。	
アカウント管理	DS-7.2	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。	
アカウント管理	DS-7.3	サービスアカウントの使用はそれを必要とするアプリケーションのみに制限します。	
アカウント管理	DS-7.4	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。	
アカウント管理	DS-7.5	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）。	
アカウント管理	DS-7.6	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。	
アカウント管理	DS-7.7	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。	
アカウント管理	DS-7.8	プロジェクトベースでコンテンツへのユーザアクセスを確認します。	
アカウント管理	DS-7.9	コンテンツを取り扱うシステム上のローカルアカウントは無効化または削除します。	

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
認証	DS-8.0	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 Identity and Access Management（AWS IAM）により、お客様は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ます。ユーザーは、AWS サービスへのアクセスに使われる独特なセキュリティ証明書を持つ（顧客の AWS アカウント内の）アイデンティティです。AWS IAM を利用すると、パスワードやアクセスキーを共有する必要がなくなり、必要に応じてユーザのアクセスを簡単に有効化または無効化することができます。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。 社内における AWS ユーザアカウント管理は ISO 27001 規格に準拠しています。AWS SOC 1 Type II レポートおよび SOC 2 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 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。
認証	DS-8.1	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。	
認証	DS-8.2	ネットワークへのリモートアクセス （例: VPN）には、2 要素認証（例: ユーザ名/パスワードおよびハードトークン）を実施します。	
認証	DS-8.3	サーバおよびワークステーションにパスワード保護されたスクリーンセーバーを導入します。	
ロギングとモニタリング	DS-9.0	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）	お客様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、およびデータに関する統制はお客様にあり、運営上、リスク上、およびコンプライアンス上の要件を満たす適切なログ管理ポリシーの実装はお客様の責任となります。 AWS では、ISO 27001 規格に基づき、ロギングおよびインシデント対応に関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 および SOC 2 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 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。
ロギングとモニタリング	DS-9.1	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。	
ロギングとモニタリング	DS-9.2	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。	
ロギングとモニタリング	DS-9.3	ログは週に 1 度確認します。	
ロギングとモニタリング	DS-9.4	コンテンツ転送に関するログを取得し、そこには以下の情報を含めるようにします。 • ユーザ名 • 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）	
ロギングとモニタリング	DS-9.5	ログは少なくとも 6 か月間保持します。	
ロギングとモニタリング	DS-9.6	ログへのアクセスは適切な関係者のみに制限します。	

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
ロギングとモニタリング	DS-9.7	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。	
セキュリティテクニック	DS-10.0	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。	お客様のデータの所有権はお客様が保持します。したがってデータの暗号化を選択するのはお客様の責任となります。 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 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。
セキュリティテクニック	DS-10.1	AES 128 ビット暗号化を用い、ハードドライブ上のコンテンツを次のいずれかの方法で暗号化します。 • 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）	
セキュリティテクニック	DS-10.2	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）。	
転送ツール	DS-11.0	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。	お客様のデータの統制と所有権はお客様が保持します。したがってデータの暗号化を選択するのはお客様の責任となります。 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 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。
転送ツール	DS-11.1	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。	
転送デバイス方法	DS-12.0	コンテンツ転送には専用のシステムを実装・使用します。	お客様のデータ、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に関する統制はお客様にあり、お客様のコンテンツ管理、およびネットワークのセグメンテーションとデータの削除に関する適切なポリシーと手順の実装はお客様の責任となります。
転送デバイス方法	DS-12.1	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。	
転送デバイス方法	DS-12.2	コンテンツ転送システムは非武装地帯（DMZ）に配置し、コンテンツ/制作ネットワークには配置しません。	
転送デバイス方法	DS-12.3	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。	

セキュリティトピック	参照番号	MPAA セキュリティベストプラクティス	MPAA ベストプラクティスに対する AWS の準拠状況
クライアントポータル	DS-13.0	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、権限を持つユーザのみに制限します。	お客様の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、および関連するすべての業務プロセス、手順、ガイドラインの所有権はお客様にあります。 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。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 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。
クライアントポータル	DS-13.1	ポータルのユーザ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。	
クライアントポータル	DS-13.2	ユーザ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）。	
クライアントポータル	DS-13.3	DMZ 内の専用サーバ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。	
クライアントポータル	DS-13.4	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。	
クライアントポータル	DS-13.5	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。	
クライアントポータル	DS-13.6	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。	
クライアントポータル	DS-13.7	クライアントポータルへのアクセスを許可する発信元 IP アドレスおよび範囲を指定して制限します。	
クライアントポータル	DS-13.8	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。	
クライアントポータル	DS-13.9	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。	
クライアントポータル	DS-13.10	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。	
クライアントポータル	DS-13.11	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: 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ています。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を提供します。 Amazon EBS ボリュームは、EC2 インスタンスの運用状況から独立した永続性を持っています。

FedRAMP: 連邦政府によるリスクと認証管理プログラム（FedRAMP）は、クラウド製品およびサービスに対するセキュリティ評価、認証、継続的なモニタリングの標準化された手法を提供します。FedRAMP 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、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指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上で、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: Identity and Access Management（IAM）は、お客様は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するものです。

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および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 27001: ISO／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。正式の仕様になることは、特定の要件が必須になることを示します。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、認定を受けることができます。

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、オブジェクトについて説明する、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 が創設した独立諮問機関であり、Payment Card Industry Data Security Standard の継続的な発展の管理を目標としています。

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（例えば EC2、S3、VPC など）。

Service Level Agreement（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 SSAE 16 レポートと呼ばれます）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

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