



アマゾン ウェブ サービス: リスクとコンプライアンス

2015 年 12 月

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

を参照してください)

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

目次

リスクとコンプライアンスの概要	3
責任共有環境.....	4
強力なコンプライアンス管理.....	5
AWS 統制の評価と統合	5
AWS の IT 統制情報.....	6
AWS のグローバルなリージョン展開	7
AWS リスクおよびコンプライアンスプログラム	7
リスク管理.....	8
統制環境.....	9
情報セキュリティ	9
AWS の認定、プログラム、レポート、およびサードパーティーによる証明	9
CJIS.....	10
CSA.....	10
Cyber Essentials Plus	11
DoD SRG レベル 2 および 4	11
FedRAMP SM	12
FERPA.....	13
FIPS 140-2.....	13
FISMA と DIACAP	14
HIPAA.....	14
IRAP	15
ISO 9001.....	16

ISO 27001	17
ISO 27017.....	19
ISO 27018	20
ITAR.....	21
MPAA.....	21
MTCS Tier 3 認定	22
NIST	22
PCI DSS レベル 1	23
SOC 1/ISAE 3402	24
SOC 2.....	26
SOC 3.....	26
コンプライアンスに関するよくある質問と AWS	26
AWS へのお問い合わせ.....	36
付録 A: CSA Consensus Assessments Initiative Questionnaire v3.0.1	37
付録 B: オーストラリア信号局 (ASD) のクラウドコンピューティングに関するセキュリティ上の 考慮事項への AWS の準拠	85
付録 C: 用語集.....	102

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

- 業界の認定と独立したサードパーティーによる証明を取得します (本文書で説明します)。
- AWS のセキュリティと統制に関する情報をホワイトペーパーおよびウェブサイトコンテンツで公表します。

- (必要に応じて) NDA に従い AWS のお客様に証明書、レポートなどの文書を直接提供します。

AWS のセキュリティの詳細については、

[AWS セキュリティセンター](https://aws.amazon.com/security/)を参照してください: <https://aws.amazon.com/security/>

AWS コンプライアンスの詳細については、

[AWS コンプライアンスのページ](https://aws.amazon.com/compliance/)を参照してください: <https://aws.amazon.com/compliance/>

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

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

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

強力なコンプライアンス管理

IT のデプロイ方法にかかわらず、AWS のお客様はこれまでどおり、IT 統制環境全体に対する適切な管理を維持することが求められます。主な作業内容として、(関連資料を基にした) 必要なコンプライアンスの目標と要件の把握、その目標と要件を満たす統制環境の構築、組織のリスク許容度に基づく必要な妥当性の把握、統制環境の運用効率の検証などがあります。AWS クラウドへのデプロイにより、企業が各種の統制や検証方法を適用するにあたって選択の幅が生まれます。

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

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

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

AWS 統制の評価と統合

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

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

AWS の IT 統制情報

AWS は、次の 2 つの方法で IT 統制情報をお客様に提供します。

1. **固有の統制定義。** AWS のお客様は、AWS が管理する主な統制を指定できます。主な統制はお客様の統制環境にとって不可欠であり、年次の会計監査などのコンプライアンス要件に準拠するには、その主な統制の運用効率について外部組織による証明が必要です。そのために、AWS は Service Organization Controls 1 (SOC 1) Type II レポートで幅広く詳細な IT 統制を公開しています。SOC 1 レポートの旧称は Statement on Auditing Standards (SAS) No. 70、Service Organizations レポートです。米国公認会計士協会 (AICPA) が作成し、幅広く認められている監査基準です。SOC 1 監査は、AWS で定義している統制目標および統制活動 (AWS が管理するインフラストラクチャの一部に対する統制目標と統制活動が含まれます) の設計と運用効率の両方に関する詳細な監査です。「Type II」は、レポートに記載されている各統制が、統制の妥当性に関して評価されるだけでなく、運用効率についても外部監査人によるテスト対象であることを示します。AWS の外部監査人は独立し、適格であるため、レポートに記載されている統制は、AWS の統制環境に高い信頼を置けることを示します。AWS の統制は、Sarbanes-Oxley (SOX) セクション 404 の財務諸表監査など、多くのコンプライアンス目的に合わせて検討され、設計され、効率的に運用することができます。SOC 1 Type II レポートの利用は、一般的に他の外部認定機関からも許可されています (たとえば、ISO 27001 の監査人は顧客の評価を完成するために SOC 1 Type II レポートを要求する場合があります)。

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

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

AWS のグローバルなリージョン展開

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。本文書の執筆時点では、リージョンは 11 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 (フランクフルト)、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)、中国 (北京)、南米 (サンパウロ) です。

AWS リスクおよびコンプライアンスプログラム

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

リスク管理

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

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

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

統制環境

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

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

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

情報セキュリティ

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

AWS の認定、プログラム、レポート、およびサードパーティーによる証明

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。



CJIS

AWS は FBI の Criminal Justice Information Services (CJIS) の基準に準拠しています。AWS では、[CJIS セキュリティポリシー](#)に基づいて必須となっている従業員の背景確認の許可および実施を含めた、CJIS セキュリティ契約をお客様と結びます。

法執行機関のお客様 (および CJIS を管理するパートナー様) も AWS の高度なセキュリティサービスおよび機能といった AWS サービスを活用して CJIS データのセキュリティと保護を向上させています。これらのサービスには、アクティビティロギング ([AWS CloudTrail](#))、使用中または保存中のデータの暗号化 (独自のキーを使用するオプションを含めた S3 のサーバー側の暗号化)、総合的なキー管理および保護 (AWS [Key Management Service](#) と [CloudHSM](#))、および統合されたアクセス権管理 (IAM フェデレーティッド認証管理、Multi-Factor Authentication) が含まれます。

AWS では、CJIS ポリシー分野に合わせたセキュリティ計画テンプレートフォーマットによる Criminal Justice Information Services (CJIS) [ワークブック](#)を作成しました。加えて、お客様のクラウド導入への道のりを支援するために CJIS ホワイトペーパーも作成しました。

CJIS ハブページにアクセス: <https://aws.amazon.com/compliance/cjis/>

CSA

2011年にクラウドセキュリティアライアンス (CSA) はクラウドプロバイダー間でセキュリティ慣行の透明性を推進するための [STAR](#) イニシアチブを立ち上げました。[CSA セキュリティ、信頼性、保証の登録](#) (STAR) は無料の一般アクセス可能な登録で、さまざまなクラウドコンピューティングサービスが提供するセキュリティコントロールが文書化されており、ユーザーが現在使用中または契約を検討中のクラウドプロバイダーのセキュリティを評価するのに役立ちます。[AWS は CSA STAR に登録しており](#)、クラウドセキュリティアライアンス (CSA) の「Consensus Assessments Initiative Questionnaire (CAIQ)」に回答済みです。CSA が発行するこの CAIQ は、どのようなセキュリティ統制が AWS の IaaS (サービスとしてのインフラストラクチャ) 内に存在するかを文書化する手段の 1 つとなっています。CAIQ には、クラウド使用者およびクラウド監査人がクラウドプロバイダーに尋ねる可能性がある 298 個の質問が記載されています。

「[付録 A: CSA Consensus Assessments Initiative Questionnaire v3.0.1](#)」を参照してください

Cyber Essentials Plus

Cyber Essentials Plus は、英国政府の支援により業界がサポートする英国発の認定スキームで、組織が一般的なサイバー攻撃に対して運用上のセキュリティを実証するのに役立ちます。

この認定は、英国政府が提供する「[10 Steps to Cyber Security \(サイバーセキュリティへの 10 ステップ\)](#)」のコンテキスト内で、一般的なインターネットベースの脅威がもたらすリスクを緩和するために AWS が実装しているベースラインコントロールを示しています。この認定は Federation of Small Businesses、Confederation of British Industry、保険会社などを含む多くの企業・業界団体が支援しており、取得したビジネスにインセンティブを提供しています。

Cyber Essentials では必要なテクニカルコントロールが示されており、関連する保証フレームワークによって、認定評価機関が毎年行う外部評価をとおして Cyber Essentials Plus 認定での独立した保証プロセスの仕組みが明らかになっています。認定は地域性が高いため、欧州 (アイルランド) リージョンに限定されています。

DoD SRG レベル 2 および 4

国防総省 (DoD) クラウドセキュリティモデル (SRG) は、クラウドサービスプロバイダー (CSP) が DoD 暫定認証を取得するための正式な評価および許可プロセスを示しており、これは DoD のお客様に使用していただくことができます。SRG の暫定認証では、AWS が DoD の基準に準拠していることを証明する再利用可能な認定が発行され、DoD ミッション所有者が該当するシステムを AWS で運用するための評価および認可に必要な時間を削減できます。AWS では現在、SRG レベル 2 および 4 で暫定認証を取得しています。

セキュリティコントロールベースラインで定義されている[レベル 2、4、5、および 6 の詳細情報については、次を参照してください: \[http://iase.disa.mil/cloud_security/Pages/index.aspx\]\(http://iase.disa.mil/cloud_security/Pages/index.aspx\)](#)。

DoD ハブページにアクセス: <https://aws.amazon.com/compliance/dod/>

FedRAMPSM

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

次のサービスは、上記のリージョンの認定範囲内に含まれます。

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

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

<https://aws.amazon.com/compliance/fedramp/>

FERPA

[The Family Educational Rights and Privacy Act](#) (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) は、学校成績書のプライバシーを保護する連邦法です。同法は、米教育省の該当するプログラムで資金援助を受けているすべての学校に適用されます。FERPA では、子供の学校成績に関する特定の権利を親に委ねています。これらの権利は、子供が 18 歳になるか、子供が高校より上のレベルの学校に通うようになると、その子供に移行されます。権利が移行された学生は「有資格学生」となります。

AWS では、FERPA が適用される該当事業者およびビジネスアソシエイトに対して、保護された学校成績情報の処理、維持、および保管について安全な AWS 環境を提供しています。

AWS では、成績データの処理や保存に AWS の活用をお考えのお客様向けに、[FERPA 関連のホワイトペーパー](#)もご用意しています。

[FERPA Compliance on AWS Whitepaper](#) は、コンプライアンスを促進するシステムを運用する方法の企業向け概要説明となっています。

https://do.awsstatic.com/whitepapers/compliance/AWS_FERPA_Whitepaper.pdf

FIPS 140-2

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

FISMA と DIACAP

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

HIPAA

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

お客様は、アカウントで HIPAA アカウントと指定された任意の AWS サービスを使用できますが、BAA で定義された HIPAA の対象サービスでのみ、PHI を処理、保存、転送できます。現在、HIPAA の対象サービスは9つあります。

- [Amazon DynamoDB](#)
- [Amazon Elastic Block Store \(EBS\)](#)
- [Amazon Elastic Cloud Compute \(EC2\)](#)
- [Elastic Load Balancing \(ELB\)](#)
- [Amazon Elastic MapReduce \(EMR\)](#)
- [Amazon Glacier](#)
- [Amazon Redshift](#)
- [Amazon Relational Database Service \(Amazon RDS\)](#)、MySQL および Oracle エンジンのみを使用
- [Amazon Simple Storage Service \(S3\)](#)

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

詳細については、HIPAA コンプライアンスに関するよくある質問を参照してください。

<https://aws.amazon.com/compliance/hipaa-compliance/>

Architecting for HIPAA Security and Compliance on Amazon Web Services:

https://do.awsstatic.com/whitepapers/compliance/AWS_HIPAA_Compliance_Whitepaper.pdf

IRAP

Information Security Registered Assessors Program (IRAP) では、オーストラリア政府の顧客が適切なコントロールを導入していることを検証でき、Australian Signals Directorate (ASD) Information Security Manual (ISM) の必要に対応した適切な責任モデルを特定するのに役立ちます。

アマゾン ウェブ サービス [では独立した評価を完了しており](#)、AWS シドニーリージョンの非機密情報 (DLM) の処理、ストレージ、および伝送において、該当するすべての ISM コントロールが導入されていることを確認しています。

IRAP 準拠のよくある質問:

<https://aws.amazon.com/compliance/irap/>

詳しくは次を参照してください。 [付録 B: オーストラリア信号局 \(ASD\) のクラウドコンピューティングに関するセキュリティ上の考慮事項への AWS の準拠](#)

ISO 9001

AWS は ISO 9001 認定を達成しており、AWS の ISO 9001 認定は AWS クラウドで品質管理された IT システムを開発、移行、運用するお客様を直接サポートします。お客様は、独自の ISO 9001 プログラムや業界別の品質プログラム (ライフサイエンスでの GxP、医療機器での ISO 13485、航空宇宙産業での AS9100、自動車産業での ISO/TS 16949 など) の取得に、AWS の準拠レポートを証拠として活用できます。品質システムの要件がないお客様にも、ISO 9001 認定により AWS の保証や透明性が向上するというメリットがあります。ISO 9001 認定は、AWS サービスと運用リージョン (下記) および次のサービスの指定された範囲の品質管理システムを対象としています。

- [AWS CloudFormation](#)
- [AWS クラウドハードウェアセキュリティモデル \(HSM\)](#)
- [Amazon CloudFront](#)
- [AWS CloudTrail](#)
- [AWS Direct Connect](#)
- [AWS Directory Service](#)
- [Amazon DynamoDB](#)
- [Amazon EC2 VM Import/Export](#)
- [AWS Elastic Beanstalk](#)
- [Amazon Elastic Block Store \(EBS\)](#)
- [Amazon Elastic Cloud Compute \(EC2\)](#)
- [Amazon EC2 Container Service \(ECS\)](#)
- [Amazon Elastic File System \(EFS\)](#)
- [Elastic Load Balancing \(ELB\)](#)
- [Amazon Elastic MapReduce \(EMR\)](#)
- [Amazon ElastiCache](#)
- [Amazon Glacier](#)
- [AWS Identity and Access Management \(IAM\)](#)
- [AWS Key Management Service \(KMS\)](#)
- [Amazon Redshift](#)
- [Amazon Relational Database Service \(RDS\)](#)
- [AWS Route 53](#)
- [Amazon SimpleDB](#)
- [Amazon Simple Email Service \(SES\)](#)
- [Amazon Simple Queue Service \(SQS\)](#)
- [Amazon Simple Storage Service \(S3\)](#)
- [AWS Storage Gateway](#)
- [Amazon Simple Workflow Service \(SWF\)](#)
- [Amazon Virtual Private Cloud \(VPC\)](#)
- [AWS WAF - ウェブアプリケーションファイアウォール](#)
- [Amazon WorkDocs](#)
- [Amazon WorkMail](#)
- [Amazon WorkSpaces](#)
- 基礎となる物理インフラストラクチャと AWS 管理環境

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

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

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

AWS ISO 9001 認定は次のウェブサイトからダウンロードできます。

https://do.awsstatic.com/certifications/iso_9001_certification.pdf

AWS は、ISO 9001 認定に関する追加情報とよくある質問を次のウェブサイトで提供しています。

<https://aws.amazon.com/compliance/iso-9001-faqs/>

ISO 27001

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

- [AWS CloudFormation](#)
- [Amazon CloudFront](#)
- [AWS Cloudtrail](#)
- [AWS Directory Service](#)
- [Amazon DynamoDB](#)
- [AWS Elastic Beanstalk](#)
- [Amazon Elastic Block Store \(EBS\)](#)

- [Amazon Elastic Cloud Compute \(EC2\)](#)
- [Amazon EC2 Container Service \(ECS\)](#)
- [AWS Direct Connect](#)
- [Amazon EC2 VM Import/Export](#)
- [AWS クラウドハードウェアセキュリティモデル \(HSM\)](#)
- [Elastic Load Balancing \(ELB\)](#)
- [Amazon Elastic File System \(EFS\)](#)
- [Amazon Elastic MapReduce \(EMR\)](#)
- [Amazon ElastiCache](#)
- [Amazon Glacier](#)
- [AWS Identity and Access Management \(IAM\)](#)
- [AWS Key Management Service \(KMS\)](#)
- [Amazon Redshift](#)
- [Amazon Relational Database Service \(RDS\)](#)
- [AWS Route 53](#)
- [Amazon SimpleDB](#)
- [Amazon Simple Email Service \(SES\)](#)
- [Amazon Simple Queue Service \(SQS\)](#)
- [Amazon Simple Storage Service \(S3\)](#)
- [Amazon Simple Workflow Service \(SWF\)](#)
- [AWS Storage Gateway](#)
- [Amazon Virtual Private Cloud \(VPC\)](#)
- [AWS WAF - ウェブアプリケーションファイアウォール](#)
- [Amazon WorkDocs](#)
- [Amazon WorkMail](#)
- [Amazon WorkSpaces](#)
- 基礎となる物理インフラストラクチャ (GovCloud を含む) と AWS 管理環境

ISO 27001/27002 は世界で広く採用されているセキュリティ基準で、会社とカスタマー情報の管理の体系的なアプローチの要件とベストプラクティスを定めるものです。これは、刻々と変化する脅威のシナリオに適する定期的リスク査定に基づいています。認定を取得するためには、会社とカスタマー情報の機密性、完全性、および可用性に影響を与える情報セキュリティリスクを管理する体系的かつ継続的なアプローチが会社にあることを示す必要があります。この認定は、セキュリティ管理や作業に関する重要情報を提供するという Amazon の取り組みを補強するものです。

AWS の ISO 27001 認定が対象となる AWS リージョンには、米国東部 (バージニア北部)、米国西部 (オレゴン)、米国西部 (北カリフォルニア)、AWS GovCloud (米国)、南米 (サンパウロ)、欧州 (アイルランド)、欧州 (フランクフルト)、アジアパシフィック (シンガポール)、アジアパシフィック (シドニー)、およびアジアパシフィック (東京) が含まれます。

AWS ISO 27001 認定は次のウェブサイトからダウンロードできます。

https://do.awsstatic.com/certifications/iso_27001_global_certification.pdf

AWS は、ISO 27001 認定に関する追加情報とよくある質問を次のウェブサイトを提供しています。

<https://aws.amazon.com/compliance/iso-27001-faqs/>

ISO 27017

ISO 27017 は国際標準化機構 (ISO) が発行する最新の行動規範です。特にクラウドサービスに関係した情報セキュリティ統制の実装ガイダンスを提供しています。

AWS は、次のものを含む AWS インフラストラクチャ、データセンター、およびサービスを対象とした Information Security Management System (ISMS) の ISO 27017 認定を達成しています。

- [Amazon CloudFront](#)
- [Amazon DynamoDB](#)
- [Amazon EC2 Container Service \(ECS\)](#)
- [Amazon Elastic Block Store \(EBS\)](#)
- [Amazon Elastic Compute Cloud \(EC2\)](#)
- [Amazon Elastic File System \(EFS\)](#)
- [Amazon Elastic MapReduce \(EMR\)](#)
- [Amazon ElastiCache](#)
- [Amazon Glacier](#)
- [Amazon Redshift](#)
- [Amazon Relational Database Service \(RDS\)](#)
- [Amazon Route 53](#)
- [Amazon Simple Email Service \(SES\)](#)
- [Amazon Simple Queue Service \(SQS\)](#)
- [Amazon Simple Storage Service \(S3\)](#)
- [Amazon Simple Workflow Service \(SWF\)](#)
- [Amazon SimpleDB](#)
- [Amazon Virtual Private Cloud \(VPC\)](#)
- [Amazon WorkDocs](#)
- [Amazon WorkMail](#)
- [Amazon WorkSpaces](#)
- [AWS CloudFormation](#)
- [AWS CloudHSM](#)
- [AWS CloudTrail](#)
- [AWS Direct Connect](#)
- [AWS Directory Service](#)
- [AWS Elastic Beanstalk](#)
- [AWS Identity and Access Management \(IAM\)](#)
- [AWS Key Management Service \(KMS\)](#)
- [AWS Storage Gateway](#)
- [AWS WAF \(ウェブアプリケーションファイアウォール\)](#)
- [Elastic Load Balancing](#)
- [VM Import/Export](#)

AWS ISO 27017 認定は次のウェブサイトからダウンロードできます。

https://do.awsstatic.com/certifications/iso_27017_certification.pdf

AWS は、ISO 27017 認定に関する追加情報とよくある質問を次のウェブサイトを提供しています。

<https://aws.amazon.com/compliance/iso-27017-faqs/>

ISO 27018

ISO 27018 は、クラウドにおける個人データの保護に焦点を当てた最初の国際的な行動規範です。ISO 情報セキュリティ基準 27002 に基づいており、パブリッククラウドにある個人を特定できる情報 (PII) に適用される ISO 27002 コントロールの導入に関するガイダンスを提供しています。また、既存の ISO 27002 コントロールセットでは対応していないパブリッククラウド PII 保護要件に対応するための追加のコントロールセットおよび関連ガイダンスも提供しています。

AWS は、次のものを含む AWS インフラストラクチャ、データセンター、およびサービスを対象とした Information Security Management System (ISMS) の ISO 27018 認定を達成しています。

- [Amazon CloudFront](#)
- [Amazon DynamoDB](#)
- [Amazon EC2 Container Service \(ECS\)](#)
- [Amazon Elastic Block Store \(EBS\)](#)
- [Amazon Elastic Compute Cloud \(EC2\)](#)
- [Amazon Elastic File System \(EFS\)](#)
- [Amazon Elastic MapReduce \(EMR\)](#)
- [Amazon ElastiCache](#)
- [Amazon Glacier](#)
- [Amazon Redshift](#)
- [Amazon Relational Database Service \(RDS\)](#)
- [Amazon Route 53](#)
- [Amazon Simple Email Service \(SES\)](#)
- [Amazon Simple Queue Service \(SQS\)](#)
- [Amazon Simple Storage Service \(S3\)](#)
- [Amazon Simple Workflow Service \(SWF\)](#)
- [Amazon SimpleDB](#)
- [Amazon Virtual Private Cloud \(VPC\)](#)
- [Amazon WorkDocs](#)
- [Amazon WorkMail](#)
- [Amazon WorkSpaces](#)
- [AWS CloudFormation](#)
- [AWS CloudHSM](#)
- [AWS CloudTrail](#)
- [AWS Direct Connect](#)
- [AWS Directory Service](#)
- [AWS Elastic Beanstalk](#)
- [AWS Identity and Access Management \(IAM\)](#)

- [AWS Key Management Service \(KMS\)](#)
- [AWS Storage Gateway](#)
- [AWS WAF \(ウェブアプリケーションファイアウォール\)](#)
- [Elastic Load Balancing](#)
- [VM Import/Export](#)

AWS ISO 27018 認定は次のウェブサイトからダウンロードできます。

https://do.awsstatic.com/certifications/iso_27018_certification.pdf

AWS は、ISO 27018 認定に関する追加情報とよくある質問を次のウェブサイトで提供しています。

<https://aws.amazon.com/compliance/iso-27018-faqs/>

ITAR

AWS GovCloud (米国) リージョンは、武器規制国際交渉規則 (**ITAR**) コンプライアンスをサポートしています。包括的な ITAR コンプライアンスプログラム管理の一環として、ITAR 輸出規制の対象となる企業は、保護されたデータへのアクセスを米国人に制限し、およびそのデータの物理的なロケーションを米国の土地に制限することによって、意図しない輸出を制御する必要があります。AWS GovCloud (米国) は、物理的に米国に位置し、そこでは AWS のスタッフによるアクセスを米国人に制限しているという環境を提供しているため、適格企業は、ITAR の規制対象となる、保護された文書およびデータを送信、処理、格納することができます。AWS GovCloud (米国) 環境は、この要件において、顧客の輸出コンプライアンスプログラムをサポートする適切な統制がなされているかどうかを検証するために、独立したサードパーティーによる監査を受けています。

MPAA

アメリカ映画協会 (MPAA) は、保護されたメディアとコンテンツを安全に保存、処理、配給するための一連のベストプラクティスをまとめました (<http://www.fightfilmtheft.org/facility-security-program.html>)。メディア企業ではこのベストプラクティスを、コンテンツとインフラストラクチャのリスクとセキュリティを評価する手段として使用しています。AWS は MPAA のベストプラクティスに準拠していることが実証されており、AWS のインフラストラクチャはすべての適用可能な MPAA インフラストラクチャコントロールに準拠しています。MPAA は「証明書」を提供していませんが、メディア業界のお客様は AWS の MPAA 型コンテンツのリスク査定および評価を補足する AWS MPAA 文書を使用することができます。

詳細については、[AWS Compliance MPAA ハブページ](#)を参照してください。

<https://aws.amazon.com/compliance/mpaa/>

MTCS Tier 3 認定

Multi-Tier Cloud Security (MTCS) とは、シンガポールで運用されているセキュリティ管理基準 (SPRING SS 584:2013) で、ISO 27001/02 情報セキュリティ管理システム (ISMS) の基準に基づいています。この認定評価では次が必要とされています。

- 企業に対する脅威や脆弱性を考慮に入れた情報セキュリティリスクの体系的な評価
- 企業とアーキテクチャに対するセキュリティリスクに対応した総合的な情報セキュリティコントロールや他の形式のリスク管理の設計および実装
- 情報セキュリティコントロールが各社の情報セキュリティの必要に継続して対応できることを保証する全体的な管理プロセスの導入

MTCS ハブページはこちらからご覧ください。

<https://aws.amazon.com/compliance/aws-multitiered-cloud-security-standard-certification/>

NIST

2015 年 6 月に、米国標準技術局 (NIST) はガイドライン **800-171**、"Final Guidelines for Protecting Sensitive Government Information Held by Contractors" を発表しました。このガイダンスは、連邦システム以外の管理指定された非機密扱いの情報 (Controlled Unclassified Information/CUI) に適用されます。

AWS は既にこれらのガイドラインに準拠しており、お客様は実質的にすぐにでも NIST 800-171 に準拠することができます。NIST 800-171 は NIST 800-53 要件のサブセットについて説明しています。このガイドラインに基づいて、AWS は FedRAMP プログラムですでに監査を受けています。FedRAMP Moderate セキュリティコントロールベースラインは 800-171 の第 3 章で言及されている推奨要件よりも厳格で、CUI データを保護する FISMA Moderate システムの要求を上回るセキュリティコントロールが数多く含まれています。詳細なマッピングについては、**[NIST Special Publication 800-171](#)**、のページ D2 (PDF 版では 37 ページ) を参照してください。

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) のレベル 1 に準拠しています。お客様は、クラウド上でクレジットカード情報を保管、処理、送信する私たちの PCI 準拠のテクノロジーインフラストラクチャ上で、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 をリリースしています。このガイドラインでは、カード保有者のデータ環境を管理しているお客様向けに、クラウドでの PCI DSS 管理作業の留意事項を記載しています。AWS では、お客様向けに PCI DSS Cloud Computing Guidelines を AWS PCI Compliance Package に組み込んでいます。AWS PCI Compliance Package には、AWS PCI Attestation of Compliance (AoC) と AWS PCI Responsibility Summary が含まれています。前者では、AWS が PCI DSS Version 3.1 においてレベル 1 サービス プロバイダに適用される標準を満たしていることが検証されています。後者では、AWS とお客様の間でコンプライアンスに関する責任をどのように分担するかが説明されています。

PCI DSS レベル 1 を対象とするサービスは次のとおりです。

- [Auto Scaling](#)
- [AWS CloudFormation](#)
- [Amazon CloudFront](#)
- [AWS CloudHSM](#)
- [AWS CloudTrail](#)
- [AWS Direct Connect](#)
- [Amazon DynamoDB](#)
- [AWS Elastic Beanstalk](#)
- [Amazon Elastic Block Store \(EBS\)](#)
- [Amazon Elastic Compute Cloud \(EC2\)](#)
- [Elastic Load Balancing \(ELB\)](#)
- [Amazon Elastic MapReduce \(EMR\)](#)
- [Amazon Glacier](#)
- [AWS Key Management Service \(KMS\)](#)
- [AWS Identity and Access Management \(IAM\)](#)
- [Amazon Redshift](#)
- [Amazon Relational Database Service \(RDS\)](#)
- [Amazon Route 53](#)
- [Amazon SimpleDB](#)
- [Amazon Simple Storage Service \(S3\)](#)
- [Amazon Simple Queue Service \(SQS\)](#)
- [Amazon Simple Workflow Service SWF](#)
- [Amazon Virtual Private Cloud \(VPC\)](#)
- 基礎となる物理インフラストラクチャ (GovCloud を含む) と AWS 管理環境

AWS PCI DSS レベル 1 認定のサービスとリージョンの最新の範囲については、次のウェブサイトを参照してください。

<https://aws.amazon.com/compliance/pci-dss-level-1-faqs/>

SOC 1/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、米国公認会計士協会 (AICPA) AT 801 (旧称 SSAE 16) および International Standards for Assurance Engagements 第 3402 号 (ISAE 3402) に従って実施されます。この 2 つの基準レポートは、米国および国際的な会計監査機関の監査における幅広い要件を満たすために作られています。SOC 1 レポートの監査は、AWS の統制目標が適切に設計されていること、およびカスタマーデータを保護するために定義された個々の統制が効果的に機能していることを証明するものです。このレポートは、監査基準書第 70 号 (SAS 70) Type II 監査レポートに代わるものです。

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

目標範囲	目標内容
セキュリティ組織	統制は、情報セキュリティポリシーが組織全体で実施され、伝達されていることについて、合理的な保証を提供するものです。
従業員ユーザーによるアクセス	統制は、Amazon 従業員ユーザーアカウントが適時に追加、変更、および削除され、定期的にレビューされるように手順が構築されていることについて、合理的な確証を提供するものです。
論理的セキュリティ	統制は、データに対する許可のない内部的および外部的アクセスを適切に制限するためのポリシーとメカニズムが用意され、顧客データが他の顧客から適切に隔離されることについて、合理的な確証を提供するものです。
安全なデータ処理	統制は、AWS ストレージの場所と顧客開始点の間のデータ処理がセキュリティで保護され、適切にマッピングされることについて、合理的な保証を提供するものです。
物理的なセキュリティと環境の予防手段	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データセンター施設に与える影響を最小限に抑えるメカニズムが存在するように、統制によって適切な保証を実現します。
変更管理	統制は、既存の IT リソースに対する変更 (緊急/特殊な設定) が記録され、認証され、試験され、承認されて文書化されることについて、合理的な保証を提供するものです。

データの完全性、 可用性および冗長性	統制は、伝送、保管、処理など、すべての段階を通じてデータの完全性が維持されることについて、合理的な保証を提供するものです。
インシデント処理	統制は、システム障害が記録、分析、および解決されることについて、合理的な保証を提供するものです。

SOC 1 レポートは、ユーザー組織の財務諸表の監査に関連する可能性が高い、サービス組織の統制を中心に設計されています。AWS の顧客基盤は広大で、AWS サービスの使用も同様に広大であるため、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う幅広い IT の一般的な統制を対象に設計されています。そのため、お客様は AWS インフラストラクチャを利用して、会計のレポートプロセスに欠かせないデータなど、重要なデータを保存および処理できます。AWS は、これらの統制の選択内容を定期的に再評価し、この重要な監査レポートのお客様のフィードバックと使用方法について考慮します。

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

- [AWS CloudFormation](#)
- [AWS CloudHSM](#)
- [AWS CloudTrail](#)
- [AWS Direct Connect](#)
- [Amazon DynamoDB](#)
- [Amazon EC2 VM Import/Export](#)
- [Amazon Elastic Beanstalk](#)
- [Amazon Elastic Block Store \(EBS\)](#)
- [Amazon ElastiCache](#)
- [Amazon Elastic Compute Cloud \(EC2\)](#)
- [Amazon Elastic Load Balancing \(ELB\)](#)
- [Amazon Elastic MapReduce \(EMR\)](#)
- [Amazon Glacier](#)
- [AWS Identity and Access Management \(IAM\)](#)
- [AWS Key Management Service \(KMS\)](#)
- [Amazon Redshift](#)
- [Amazon Relational Database Service \(RDS\)](#)
- [Amazon Route 53](#)
- [Amazon SimpleDB](#)
- [Amazon Simple Email Service \(SES\)](#)
- [Amazon Simple Storage Service \(S3\)](#)
- [Amazon Simple Workflow \(SWF\)](#)
- [Amazon Simple Queue Service \(SQS\)](#)
- [AWS Storage Gateway](#)
- [Amazon Virtual Private Cloud \(VPC\)](#)
- [Amazon WorkSpaces](#)

SOC 2

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

SOC 3

AWS は Service Organization Controls 3 (SOC 3) レポートを発行しています。SOC 3 レポートは、AWS SOC 2 レポートを一般公開用に要約したものです。レポートには、(SOC 2 レポートに含まれる [AICPA の Security Trust Principles](#) に基づく) 管理の操作の外部監査人の意見、制御の有効性に関する AWS マネジメントからの表明、AWS インフラストラクチャおよびサービスの概要が含まれます。AWS SOC 3 レポートには、対象サービスをサポートする目標のサービスをサポートする世界中の AWS データセンターすべてを含みます。これは SOC 2 レポートを請求する手続きを踏まなくとも、AWS が外部監査人の保証を得ていることを確認できる便利な資料です。SOC 3 レポートの範囲には、SOC 1 レポートの対象と同じサービスが含まれます。対象となるサービスの詳細については上記の SOC 1 の説明を参照してください。 [AWS SOC 3 レポートはこちらからご覧ください。](#)

コンプライアンスに関するよくある質問と AWS

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

参照番号	クラウドコンピューティングに関する質問	AWS の情報
1	統制の所有権。クラウドにデプロイしたインフラストラクチャを統制する所有権は誰にありますか？	AWS にデプロイされている部分については、AWS がそのテクノロジーの物理コンポーネントを統制します。その他の部分は、接続ポイントや送信の統制を含め、お客様がすべてを所有し、統制します。AWS で定めている統制の内容と、効率的に運用する方法について理解できるように、AWS では SOC 1 Type II レポートを発行し、EC2、S3、VPC を中心とした定義済みの統制、ならびに詳細な物理セキュリティおよび環境統制を公表しています。これらの統制の定義は、ほとんどのお客様のニーズを満たします。AWS と機密保持契約を結んでいる AWS のお客様は、SOC 1 Type II レポートのコピーを要求できます。
2	IT の監査。クラウドプロバイダーの監査はどのように実施すればよいですか？	ほとんどのレイヤーと、物理統制よりも上の統制の監査は、お客様の担当です。AWS 定義の論理統制と物理統制の定義は、SOC 1 Type II レポートに文書化されています。また、このレポートは、この監査チームとコンプライアンスチームのレビューに使用できます。また、AWS ISO 27001 およびその他の認定も、監査人のレビュー用に使用できます。
3	Sarbanes-Oxley への準拠。対象のシステムがクラウドプロバイダー環境にデプロイされている場合、SOX への準拠はどのように達成されますか？	お客様が AWS クラウドで会計情報を処理する場合、AWS システムの一部を Sarbanes-Oxley (SOX) の要件の範囲に組み込むことについては、お客様の監査人が判断してください。お客様の監査人は、SOX の適用可能性について独自に判断する必要があります。ほとんどの論理アクセス統制はお客様が管理するため、関連する基準に統制活動が適合しているかどうかは、お客様が判断されるのが最適です。SOX 監査人が AWS の物理的統制に関する詳細情報を必要とする場合は、AWS の SOC 1 Type II レポートを参照できます。AWS が提供する統制が詳細に記載されています。

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
4	HIPAA への準拠。クラウドプロバイダー環境にデプロイしている場合でも、HIPAA のコンプライアンス要件を満たすことができますか？	HIPAA 要件は AWS のお客様に適用され、AWS のお客様が統制します。AWS プラットフォームでは、HIPAA などの業界固有の認定要件を満たすソリューションのデプロイが可能です。お客様は AWS のサービスを利用することで、電子健康記録を保護するために必要な要件以上のセキュリティレベルを維持できます。HIPAA のセキュリティおよびプライバシーに関する規則に準拠したヘルスケアアプリケーションが、お客様によって AWS 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ー環境にデプロイしている場合でも、GLBA の認定要件を満たすことができますか？	ほとんどの GLBA 要件は、AWS のお客様が統制します。AWS は、データの保護、アクセス許可の管理、および AWS インフラストラクチャでの GLBA 準拠アプリケーションの構築をお客様が行うための手段を提供しています。物理セキュリティ統制が効率的に運用されている具体的な保証が必要な場合は、必要に応じて AWS SOC 1 Type II レポートを参照できます。
6	米国連邦規制への準拠。米国政府機関がクラウドプロバイダ環境にデプロイしている場合に、セキュリティおよびプライバシーの規制に準拠することはできますか？	米国連邦機関は、2002 年施行の連邦情報セキュリティマネジメント法 (FISMA)、Federal Risk and Authorization Management Program (FedRAMP SM)、Federal Information Processing Standard (FIPS) 出版物 140-2、武器規制国際交渉規則 (ITAR) など、数多くのコンプライアンス基準に準拠することができます。また、該当する法律に規定されている要件に応じて、他の法律や状況への準拠も達成できる場合があります。

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
7	データの場所。ユーザーデータはどこにありますか?	データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。S3 データオブジェクトのデータレプリケーションは、データが保存されているリージョンのクラスタ内で実行され、他のリージョンの他のデータセンタークラスタにはレプリケートされません。データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しないものとします。本文書の執筆時点では、リージョンは 11 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 (フランクフルト)、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)、中国 (北京)、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。たとえば、オペレーティングシステム、ネットワーク構成、インストールされているアプリケーションなどです。お客様は、AWS を使用して保存または処理する電子文書の特定、収集、処理、分析、および作成に関連する法的手続きに、適切に対応する責任を持ちます。法的手続きに AWS の協力を必要とするお客様には、AWS は要請に応じて連携をとります。

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

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
12	内部者によるアクセス。クラウドプロバイダは、ユーザーのデータとアプリケーションに対する内部者による不適切なアクセスの脅威に対処していますか？	AWS は、内部者による不適切なアクセスの脅威に対処するための SOC 1 統制を提供しています。また、本文書で説明している公開認定およびコンプライアンスの取り組みにより、内部者によるアクセスに対処しています。すべての認定とサードパーティーによる証明で、論理アクセスの予防統制と検出統制が評価されています。さらに、定期的なリスク評価時に、内部者によるアクセスの統制および監視方法を評価しています。
13	マルチテナント。ユーザーの分離は安全に実施されていますか？	AWS 環境は仮想化されたマルチテナント環境です。AWS は、お客様間を他のお客様から隔離するように設計されたセキュリティ管理プロセス、PCI 統制などのセキュリティ統制を実施しました。AWS システムは、仮想化ソフトウェアによるフィルタ処理によって、お客様に割り当てられていない物理ホストや物理インスタンスにアクセスできないように設計されています。このアーキテクチャは独立 PCI 認定審査機関 (QSA) によって検証済みで、2015 年 4 月に発行された PCI DSS 3.1 版のすべての要件に準拠することが確認されています。 また、AWS にはシングルテナントのオプションもあります。ハードウェア専用インスタンスは、単一のお客様専用のハードウェアを実行する Amazon Virtual Private Cloud (Amazon VPC) で起動される Amazon EC2 インスタンスです。専用インスタンスを使用することで、Amazon VPC および AWS クラウドの利点をフルに活用しながら、Amazon EC2 インスタンスをハードウェアレベルで隔離できます。

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
14	ハイパーバイザーの脆弱性。クラウドプロバイダーは、ハイパーバイザー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 ハイパーバイザーを利用しています。ハイパーバイザーは、社内および社外の侵害対策チームによって新規および既存の脆弱性と攻撃進路を定期的に評価しています。また、ゲスト仮想マシン間の強力な隔離を維持するためにも適しています。AWS Xen ハイパーバイザーのセキュリティは、評価および監査の際に独立監査人によって定期的に評価されています。Xen ハイパーバイザーおよびインスタンスの隔離の詳細については、AWS セキュリティホワイトペーパーをご覧ください。
15	脆弱性の管理。システムには適切にパッチが適用されていますか？	AWS は、ハイパーバイザーおよびネットワークサービスなど、お客様へのサービス提供をサポートするシステムにパッチを適用する責任を持ちます。この処理は、AWS ポリシーに従い、また ISO 27001、NIST、および PCI の要件に準拠して、必要に応じて実行します。お客様が使用しているゲストオペレーティングシステム、ソフトウェア、およびアプリケーションの統制については、お客様が行い、お客様がそれらのシステムにパッチを適用する責任を持ちます。
16	暗号化。提供されているサービスは暗号化をサポートしていますか？	はい。AWS では、S3、EBS、SimpleDB、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC への IPsec トンネルも暗号化されます。また、Amazon S3 は、お客様向けのオプションとしてサーバー側の暗号化も提供しています。お客様は、サードパーティーの暗号化テクノロジーを使用することもできます。詳細については、AWS セキュリティホワイトペーパーを参照してください。

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
17	データの所有権。クラウドプロバイダー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ーはユーザーデータを適切に隔離していますか？	AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。Amazon S3 は高度なデータアクセス統制を提供しています。具体的なデータサービスのセキュリティの詳細については、AWS セキュリティホワイトペーパーをご覧ください。
19	複合サービス。クラウドプロバイダのサービスは、他のプロバイダのクラウドサービスをベースに利用していますか？	AWS はお客様に AWS サービスを提供するにあたり、サードパーティーのクラウドプロバイダー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ーによって運営されていますか？	はい。これらの統制は、SOC 1 Type II レポートに具体的に記載されています。さらに、ISO 27001 や FedRAMP sm など、AWS がサポートするその他の認定では、ベストプラクティスの物理統制や環境統制が必要です。
21	クライアント側の保護。クラウドプロバイダーでは、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。

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
22	サーバーのセキュリティ。クラウドプロバイダーでは、仮想サーバーをユーザーが保護できますか？	はい。AWS では、お客様独自のセキュリティアーキテクチャを実装できます。サーバーおよびネットワークのセキュリティの詳細については、AWS セキュリティホワイトペーパーをご覧ください。
23	Identity and Access Management。サービスに IAM 機能は含まれますか？	AWS には Identity and Access Management (IAM) サービスシリーズがあるので、お客様は、ユーザー ID の管理、セキュリティ認証情報の割り当て、ユーザーのグループ化による整理、およびユーザーのアクセス許可の管理を一元的に行うことができます。詳細については、AWS ウェブサイトをご覧ください。
24	保守による停止の予定。プロバイダーは、保守のためにシステムを停止する予定を指定していますか？	AWS では、定期的な保守やシステムのパッチ適用を実行するために、システムをオフラインにする必要がありません。通常、AWS の保守およびシステムのパッチ適用はお客様に影響がありません。インスタンスの保守自体は、お客様が統制します。
25	拡張機能。ユーザーが元々の契約を超えて拡張することを許可していますか？	AWS クラウドは分散され、セキュリティと復元力が高いので、潜在的に大きな拡張性があります。お客様は、使用内容に対する料金のみを支払って、拡張または縮小できます。
26	サービスの可用性。高レベルの可用性を確約していますか？	AWS は、サービスレベルアグリーメント (SLA) で高レベルの可用性を確約しています。たとえば、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	分散型サービス妨害 (DDoS) 攻撃。DDoS 攻撃に対してサービスをどのように保護していますか？	AWS ネットワークは、既存のネットワークセキュリティの問題に対する強固な保護機能を備えており、お客様はさらに堅牢な保護を実装することができます。DDoS 攻撃の説明などの詳細については、AWS セキュリティホワイトペーパーをご覧ください。

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
28	データの可搬性。サービスプロバイダーに保存されているデータは、ユーザーが依頼すればエクスポートできますか?	AWS では、必要に応じてお客様がデータを AWS ストレージから出し入れすることを許可しています。S3 用 AWS Import/Export サービスでは、転送用のポータブル記憶装置を使用して、AWS 内外への大容量データの転送を高速化できます。
29	サービスプロバイダのビジネス継続性。ビジネス継続性プログラムがありますか?	AWS では、ビジネス継続性プログラムを運用しています。詳細な情報については、AWS セキュリティホワイトペーパーをご覧ください。
30	ユーザーのビジネス継続性。ユーザーがビジネス継続性計画を実装することはできますか?	AWS は、堅牢な継続性計画を実装する機能をお客様に提供しています。たとえば、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/アベイラビリティゾーンでのデプロイアーキテクチャなどです。
31	データの耐久性。サービスでは、データの耐久性を規定していますか?	Amazon S3 は極めて堅牢性の高いストレージインフラストラクチャを提供しています。オブジェクトは冗長化のため、同一の Amazon S3 リージョン内の複数施設に分散した複数のデバイスに保存されます。一旦格納されると、Amazon S3 は冗長性が失われた場合にすばやく検出して修復することによってオブジェクトの堅牢性を維持します。Amazon S3 は、チェックサムを用いて、格納されているデータの完全性を定期的に検証しています。破損が検出されると、冗長データを使用して修復されます。S3 に保存されるデータは、1 年間にオブジェクトの 99.999999999% の堅牢性と 99.9% の可用性を提供するよう設計されています。

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
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ーを使用してテープへのバックアップを実行することを許可しています。ただし、AWS ではテープへのバックアップサービスを提供していません。Amazon S3 サービスはデータ損失の可能性をほぼ 0% にまで低減する設計になっており、データストレージの冗長化によってデータオブジェクトのマルチサイトコピーに匹敵する永続性を実現しています。データの永続性と冗長性については、AWS のウェブサイトをご覧ください。
33	値上げ。突然値上げを行うことがありますか？	AWS には、サービス提供のコストが徐々に下がるにつれて、料金を頻繁に下げてきた歴史があります。ここ数年間でも、継続的に値下げを行っています。
34	持続可能性。サービスプロバイダー会社には、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ーであり、Amazon.com の長期ビジネス戦略です。AWS には、非常に長期間の持続可能性があります。

AWS へのお問い合わせ

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

付録 A: CSA Consensus Assessments Initiative Questionnaire

v3.0.1

クラウドセキュリティアライアンス (Cloud Security Alliance/CSA) は、「クラウドコンピューティング内のセキュリティ保証を提供するためのベストプラクティスの使用を促進し、クラウドコンピューティングの使用に関する教育を提供して、あらゆる形式のコンピューティングの保護を支援する目的を持つ非営利組織」です。

[参照先: <https://cloudsecurityalliance.org/about/>] この目標を達成するために、幅広い業界のセキュリティの専門家、会社、および団体がこの組織に参加しています。

CSA Consensus Assessments Initiative Questionnaire には、クラウド使用者およびクラウド監査人がクラウドプロバイダーに要求すると 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ーの選択やセキュリティの評価など、幅広い用途に使用できます。AWS はこの調査票に回答済みです。内容は以下のとおりです。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
アプリケーション および インターフェイス セキュリティ アプリケーション のセキュリティ	AIS-01.1	業界基準 (Build Security in Maturity Model [BSIMM] Benchmarks、Open Group ACS Trusted Technology Provider Framework、NIST など) を利用して、システム /ソフトウェア開発ライフサイクル (Systems/Software Development Lifecycle/SDLC) のセキュリティに組み込んでいますか?	AWS のシステム開発ライフサイクルは、業界のベストプラクティスを組み込んでおり、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスク評価の完遂などが含まれています。詳細については、AWS セキュリティプロセスの概要を参照してください。 AWS は、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。詳細については、ISO 27001 基準の付録 A、ドメイン 14 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。
	AIS-01.2	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?	
	AIS-01.3	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、手動ソースコード分析ツールを利用していますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	AIS-01.4	すべてのソフトウェアサブライヤが、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?	
	AIS-01.5	(SaaS のみ) アプリケーションにセキュリティの脆弱性がないことを確認し、問題があれば本番での導入前に対処しますか?	
アプリケーション および インターフェイス セキュリティ 顧客 のアクセス要件	AIS-02.1	データ、資産、および情報システムに対するアクセス権を顧客に付与する前に、顧客のアクセスに関するすべての特定されたセキュリティ、契約、および規制の要件には契約によって対応および改善されていますか?	AWS のお客様は、適用可能な法律および規制に準拠する範囲で AWS を使用する責任を有しています。AWS は、業界の認定およびサードパーティーによる証明、ホワイトペーパー (http://aws.amazon.com/compliance で入手可能) 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。
	AIS-02.2	お客様のアクセスに関するすべての要件および信頼レベルは定義および文書化されていますか?	
アプリケーション および インターフェイス セキュリティ データの完全性	AIS-03.1	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イスおよびデータベースについてデータの入力と出力の整合性ルーチン (一致チェック、編集チェックなど) が実装されていますか?	AWS のデータ整合性統制は AWS SOC 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整合性統制が維持されることを示しています。 また、詳細については、ISO 27001 基準の付録 A、ドメイン 14 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。
アプリケーション および インターフェイス セキュリティ データの セキュリティと 完全性	AIS-04.1	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 (CDSA、MULITSAFE、CSA Trusted Cloud Architectural Standard、FedRAMP、CAESARS など)?	AWS Data Security Architecture は、業界の主要な慣例を組み込むように設計されています。 AWS が準拠するさまざまな主要な慣行の詳細については、AWS 認定、レポート、およびホワイトペーパーを参照してください (http://aws.amazon.com/compliance で入手可能)。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
監査の保証と コンプライアンス 監査の計画	AAC-01.1	構造化された、業界で受け入れられている形式 (CloudAudit/A6 URI Ontology、CloudTrust、SCAP/CYBEX、GRC XML、ISACA の Cloud Computing Management Audit/Assurance Program など) を使用して、監査要点を作成していますか?	AWS は、いくつかの業界の認定と独立したサードパーティーによる証明を取得し、いくつかの認定、レポートなどの関連する文書を AWS のお客様に直接提供しています。
監査の保証と コンプライアンス 独立監査	AAC-02.1	テナントに対して、自社の SOC2/ISO 27001 または同様のサードパーティー監査または認定レポートを見ることを許可していますか?	AWS は、サードパーティーによる証明、認定、Service Organization Controls (SOC) 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 ISO 27001 認定は次のウェブサイトからダウンロードできます。 http://do.awsstatic.com/certifications/iso_27001_global_certification.pdf AWS SOC 3 レポートは次のウェブサイトからダウンロードできます。 https://do.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf
	AAC-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行っていますか?	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はスキャンします (お客様のインスタンスはこのスキャンの対象外です)。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、脆弱性に対する外部からの脅威の査定が、独立系のセキュリティ会社によって定期的に行われます。これらの査定に起因する発見や推奨事項は、分類整理されて AWS 上層部に報告されます。
	AAC-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行っていますか?	さらに、AWS 統制環境は、通常の内部的および外部的監査およびリスク評価によって規定されています。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。
	AAC-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行っていますか?	
	AAC-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行っていますか?	
	AAC-02.6	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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	AAC-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?	
	AAC-02.8	評価の機能横断型監査が可能な内部監査プログラムを実施していますか?	
監査の保証と コンプライアンス 情報システムの 規制マッピング	AAC-03.1	顧客データを論理的にセグメント化または暗号化することで、別のテナントのデータに不注意でアクセスすることなく単一のテナントに対してのみデータを作成することができますか?	AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。お客様が自身のデータの統制と所有権を有しているため、データの暗号化を選択するのはお客様の責任です。AWS では、S3、EBS、SimpleDB、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC への IPsec トンネルも暗号化されます。加えて、お客様は AWS Key Management Systems (KMS) を活用して暗号化キーの作成と管理を行えます (https://aws.amazon.com/kms/ を参照)。詳細については、次のウェブサイトです入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。 http://aws.amazon.com/security
	AAC-03.2	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?	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ーを使用してテープへのバックアップを実行することを許可しています。ただし、AWS ではテープへのバックアップサービスを提供していません。Amazon S3 および Glacier 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。
	AAC-03.3	特定の国や地理的な場所に顧客データの保存を制限する能力がありますか?	AWS のお客様は、コンテンツ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。本文書の執筆時点では、リージョンは 11 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)、欧州 (フランクフルト)、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)、中国 (北京)、南米 (サンパウロ) です。
	AAC-03.4	該当する管轄区域での規制変更の監視、法的要件の変更に応じたセキュリティプログラムの調整、および該当する規制要件への準拠の保証に対応したプログラムを導入していますか?	AWS では、該当する法律、契約、規制による要件を監視しています。 詳細については、ISO 27001 基準の付録 18 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。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
ビジネス継続性の 管理と運用の耐障 害性	BCR-01.1	地理的に弾力性のあるホス 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。
ビジネス継続性の 計画	BCR-01.2	インフラストラクチャサー ビスを他のプロバイダーに 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?	顧客は AWS の使用量を計画しながら、複数のリージョンやアベイラビリティ ゾーンを利用する必要があります。 詳細については、次のウェブサイトで入手可能な AWS クラウドセキュリティホワ イトペーパーの概要を参照してください。 http://aws.amazon.com/security 。
ビジネス継続性の 管理と運用の耐障 害性	BCR-02.1	ビジネス継続性計画の効果 を継続させるために、スケ ジュールした間隔で、また は重大な組織または環境の 変更時に、計画はテストさ れますか?	AWS のビジネス継続性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 17 を参照してください。
ビジネス継続性の 管理と運用の耐障 害性	BCR-03.1	システム間のデータのトラ ンスポート経路を示す文書 を、テナントに提供してい ますか?	データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。 AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客 様に通知することなく、お客様が選択したリージョンからサービス利用者コンテン ツを移動しないものとします。詳細については AWS SOC 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。
電力および 電気通信	BCR-03.2	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?	
ビジネス継続性の 管理と運用の耐障 害性	BCR-04.1	情報システムの設定、イン ストール、および運用を行 うための情報システムの文 書 (管理者およびユーザーガ イド、アーキテクチャ図な ど) は、権限のある担当者が 利用できるようにしていま すか?	情報システムの文書は、Amazon のイントラネットサイトを使用して AWS 社内の担 当者が使用できるようにしています。詳細については、次のウェブサイトで入手可 能な AWS クラウドセキュリティホワイトペーパーを参照してください。 http://aws.amazon.com/security/ 。 詳細については、ISO 27001 付録 A、ドメイン 12 を参照してください。
ビジネス継続性の 管理と運用の耐障 害性	BCR-05.1	破損 (自然の原因、災害、意 図的な攻撃などによる) 対 する物理的な保護が予測お よび設計され、対策が適用 されていますか?	AWS のデータセンターは、環境リスクに対する物理的な保護を組み込んでいます。環 境リスクに対する AWS の物理的な保護は、独立監査人によって検証され、 ISO 27002 のベストプラクティスに準拠していると認定されました。 詳細については、ISO 27001 基準の付録 A、ドメイン 11 を参照してくだ さい。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
ビジネス継続性の 管理と運用の耐障 害姓 設備の場所	BCR-06.1	いずれかのデータセンターが、影響の大きい環境リスク (洪水、竜巻、地震、台風など) が頻繁に発生する、または発生する可能性が高い場所にありますか?	AWS のデータセンターは、環境リスクに対する物理的な保護を組み込んでいます。環境リスクに対する AWS の物理的な保護は、独立監査人によって検証され、ISO 27002 のベストプラクティスに準拠していると認定されました。詳細については、ISO 27001 基準の付録 A、ドメイン 11 を参照してください。
ビジネス継続性の 管理と運用の耐障 害姓 設備の保守	BCR-07.1	仮想インフラストラクチャを使用している場合、クラウドソリューションには、ハードウェアに依存しない復元機能と修復機能が含まれますか?	お客様は EBS Snapshot 機能を使用して、いつでも仮想マシンイメージをキャプチャし、復元できます。お客様は、AMI をエクスポートして、施設内または別のプロバイダーで使用できます (ただし、ソフトウェアのライセンス制限に従います)。詳細については、次のウェブサイトですぐ入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。 http://aws.amazon.com/security 。
	BCR-07.2	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?	
	BCR-07.3	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ーに移植することを許可していますか?	
	BCR-07.4	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?	
	BCR-07.5	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ーに依存しない復元機能および修復機能が含まれますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
ビジネス継続性の 管理と運用の耐障 害姓 設備の電源障害	BCR-08.1	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 基準に合わせて公共サービスの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 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 クラウドセキュリティホワイトペーパー (http://aws.amazon.com/security) を参照してください。
ビジネス継続性の 管理と運用の耐障 害姓 影響の分析	BCR-09.1	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?	AWS CloudWatch は、AWS 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のモニタリングを提供します。詳細については、 aws.amazon.com/cloudwatch を参照してください。また、AWS は、サービス状態ダッシュボード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。
	BCR-09.2	基準に基づく情報セキュリティメトリックス (CSA、CMMI など) をテナントが利用できるようにしていますか?	
	BCR-09.3	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?	
ビジネス継続性の 管理と運用の耐障 害姓 ポリシー	BCR-10.1	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 セキュリティフレームワークは、NIST 800-53、ISO 27001、ISO 27017、ISO 27018、ISO 9001 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 リスクとコンプライアンスホワイトペーパー (http://aws.amazon.com/compliance で入手可能) を参照してください。
ビジネス継続性の 管理と運用の耐障 害姓 保持ポリシー	BCR-11.1	テナントデータの保持ポリシーを実施するための技術的な統制機能はありますか?	AWS は、お客様に対して、お客様のデータを削除する機能を提供しています。ただし、AWS のお客様は、お客様のデータの統制と所有権を有していますので、お客様の要件に応じてデータの保持を管理するのはお客様の責任です。詳細については、次のウェブサイトで入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。 http://aws.amazon.com/security/ 。 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。その他の情報については、 https://aws.amazon.com/compliance/data-privacy-faq/ を参照してください。
	BCR-11.2	政府またはサードパーティー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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	BCR-11.4	規制、法令、契約、またはビジネス要件へのコンプライアンスを保証するためのバックアップまたは冗長性メカニズムを導入していますか?	AWS のバックアップおよび冗長性メカニズムは、ISO 27001 基準に合わせて開発され、テストされています。AWS のバックアップおよび冗長性メカニズムに関する追加情報については、ISO 27001 基準の付録 A、ドメイン 12 および AWS SOC 2 レポートを参照してください。
	BCR-11.5	バックアップまたは冗長性メカニズムを少なくとも毎年 1 回はテストしますか?	
変更コントロール と設定管理 新規開発および 獲得	CCC-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 セキュリティフレームワークは、NIST 800-53、ISO 27001、ISO 27017、ISO 27018、ISO 9001 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。 お客様が初めて AWS を使う場合でも、または高度なユーザーでも、基本の紹介から高度な機能にいたるサービス関連の有益な情報が https://aws.amazon.com/documentation/ のウェブサイトにある「AWS ドキュメント」セクションに掲載されています。
	CCC-01.2	製品/サービス/機能の実装、構成、および使用について説明したドキュメントが利用可能ですか?	
変更コントロール と設定管理 外注による開発	CCC-02.1	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、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 12 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。
	CCC-02.2	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?	
変更コントロール と設定管理 品質テスト	CCC-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 9001 認定を維持しています。これは AWS 品質システムの独立した検証であり、AWS のアクティビティが ISO 9001 の要件に準拠していることを示しています。 AWS Security Bulletins では、セキュリティおよびプライバシーに関するイベントについてお客様に通知しています。お客様は AWS Security Bulletin の RSS フィードにウェブサイトから登録できます。 aws.amazon.com/security/security-bulletins/ を参照してください。
	CCC-03.2	特定の製品/サービスに関する既知の問題を説明したドキュメントが入手可能ですか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	CCC-03.3	提供される製品やサービスに関して報告されたバグやセキュリティの脆弱性について、優先順位付けを行い、修正するためのポリシーおよび手順を設けていますか?	<p>また、AWS は、サービス状態ダッシュボード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。</p> <p>AWS のシステム開発ライフサイクル (SDLC) 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 セキュリティプロセスの概要を参照してください。</p>
	CCC-03.4	リリースされたソフトウェアバージョンからすべてのデバッグおよびテストコード要素が取り除かれていることを保証するためのメカニズムが設けられていますか。	また、詳細については、ISO 27001 基準の付録 A、ドメイン 14 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。
変更コントロールと設定管理 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	CCC-04.1	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?	<p>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。</p> <p>詳細については、ISO 27001 基準の付録 A、ドメイン 12 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。</p>
変更コントロールと設定管理 運用の変更	CCC-05.1	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?	<p>AWS SOC レポートには、AWS 環境における管理体制を変更する際の統制の概要が記載されています。</p> <p>また、詳細については、ISO 27001 基準の付録 A、ドメイン 14 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。</p>
データセキュリティと情報ライフサイクル管理 分類	DSI-01.1	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 (たとえば、タグを使用して、ゲストオペレーティングシステムが不適切な国で起動、データのインスタンス化、データの転送を実行しないように制限することなどができますか)?	仮想マシンは、EC2 サービスの一部としてお客様に割り当てられています。お客様は、使用されるリソースとリソースの場所に関する統制を有しています。詳細については、AWS のウェブサイト (http://aws.amazon.com) を参照してください。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	DSI-01.2	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 (たとえば、TXT/TPM、VN-Tag など)?	AWS は、EC2 リソースにタグを設定する機能を提供しています。メタデータの 1 形式である EC2 タグは、ユーザーが親しみやすい名前の作成、検索性の強化、および複数ユーザー間の協調の改善に使用できます。また、AWS マネジメントコンソールは、タグ付けもサポートしています。
	DSI-01.3	1 つの認証要素としてシステムの地理的位置を使用する機能はありますか?	AWS は、IP アドレスに基づく条件付きユーザーアクセスの機能を提供しています。お客様は条件を追加して、時刻、その発信元の IP アドレス、SSL を使用するかどうかなど、ユーザーがどのように AWS を使用するかをコントロールできます。
	DSI-01.4	依頼に応じて、テナントのデータが格納されている場所の物理的な位置または地理を提供していますか?	AWS は、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しないものとします。本文書の執筆時点では、リージョンは 11 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)、欧州 (フランクフルト)、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)、中国 (北京)、南米 (サンパウロ) です。
	DSI-01.5	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事前に提供していますか?	AWS は、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しないものとします。本文書の執筆時点では、リージョンは 11 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)、欧州 (フランクフルト)、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)、中国 (北京)、南米 (サンパウロ) です。
	DSI-01.6	構造化データラベリング基準 (ISO 15489、Oasis XML Catalog Specification、CSA データタイプガイダンスなど)に従っていますか?	AWS のお客様は、お客様のデータの統制と所有権を有しています。また、お客様の要件に合う構造化データラベリング基準を実装することができます。
	DSI-01.7	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?	AWS は、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しないものとします。本文書の執筆時点では、リージョンは 11 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)、欧州 (フランクフルト)、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)、中国 (北京)、南米 (サンパウロ) です。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
データセキュリティと情報ライフサイクル管理 データインベントリおよびフロー	DSI-02.1	サービスのアプリケーションとインフラストラクチャネットワークおよびシステム内にあるデータ (永続的または一時的) のデータフローのインベントリ、文書化、および維持を行っていますか?	AWS のお客様は、コンテンツ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。本文書の執筆時点では、リージョンは 11 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)、欧州 (フランクフルト)、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)、中国 (北京)、南米 (サンパウロ) です。
	DSI-02.2	定義された地理的保管場所の外にデータが移動しないことを保証できますか?	
データセキュリティと情報ライフサイクル管理 e コマーストランザクション	DSI-03.1	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移動する必要がある場合に (インターネットなど)、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?	すべての AWS API は、サーバー認証を提供する、SSL で保護されたエンドポイント経由で利用可能です。AWS では、S3、EBS、SimpleDB、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC への IPSec トンネルも暗号化されます。加えて、お客様は AWS Key Management Systems (KMS) を活用して暗号化キーの作成と管理を行えます (https://aws.amazon.com/kms/ を参照)。お客様は、サードパーティーの暗号化テクノロジーを使用することもできます。 詳細については、次のウェブサイトですぐ入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。 http://aws.amazon.com/security 。
	DSI-03.2	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経由で相互に通信する必要がある場合 (例: 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?	
データセキュリティと情報ライフサイクル管理 処理、ラベリング、セキュリティポリシー	DSI-04.1	データおよびデータを含むオブジェクトのラベリング、処理、およびセキュリティに関するポリシーおよび手続きが規定されていますか?	AWS のお客様は、お客様のデータの統制と所有権を有しています。また、お客様は、お客様の要件に合うラベリングおよび処理に関するポリシーおよび手続きを実装できます。
	DSI-04.2	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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
データセキュリティと情報ライフサイクル管理 非運用データ	DSI-05.1	運用データが非運用環境にレプリケートされたり、使用されたりすることを禁止する手順がありますか？	AWS のお客様は、お客様のデータの統制と所有権を有しています。AWS は、お客様が運用環境および非運用環境を保守および開発できるようにしています。運用データが非運用環境にレプリケートされないようにするのは、お客様の責任です。
データセキュリティと情報ライフサイクル管理 所有権および財産管理	DSI-06.1	データの財産管理に関する責任を定義し、割り当て、文書化し、通知していますか？	AWS のお客様は、お客様のデータの統制と所有権を有しています。詳細については、AWS カスタマーアグリーメントを参照してください。
データセキュリティと情報ライフサイクル管理 安全な廃棄	DSI-07.1	テナントの決定による、アーカイブまたはバックアップ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？	<p>AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M (国家産業セキュリティプログラム運営マニュアル) または NIST 800-88 (媒体のサニタイズに関するガイドライン) に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。詳細については、次のウェブサイト入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。 http://aws.amazon.com/security/</p> <p>Amazon EBS ボリュームは、ワイプ処理を行った後、未フォーマットのローブロックデバイスとしてお客様に提供されます。ワイプは再使用の直前に実施されるため、お客様に提供された時点でワイプ処理は完了しています。業務手順上、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」) や NIST 800-88 (「媒体のサニタイズに関するガイドライン」) が指定するような、特定の手法で全データをワイプする必要がある場合、お客様自身で Amazon EBS のワイプ作業を行うこともできます。お客様がしかるべき手順でワイプを実施してからボリュームを削除することで、コンプライアンスの要件を満たすようにします。</p> <p>機密データの暗号化は、一般的なセキュリティのベストプラクティスです。AWS には、EBS ボリュームとスナップショットを AES-256 で暗号化する機能があります。EC2 インスタンスをホストするサーバーで暗号化が行われるため、EC2 インスタンスと EBS ストレージとの間で移動するデータが暗号化されます。この処理が効率的に低レイテンシーで行われるようにするために、EBS 暗号化機能は EC2 の強力なインスタンスタイプ (たとえば、M3、C3、R3、G2) だけで使用できます。</p>

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	DSI-07.2	サービス手配の終了に関する手順を公開できますか? たとえば、顧客が環境の利用を終了した場合やリソースを無効にした場合に、テナントデータのコンピューティングリソースすべてを消去する保証などです。	
データセンター セキュリティ 資産管理	DCS-01.1	資産の所有権を含めて、すべての重要資産の一覧表を保守していますか?	ISO 27001 基準に合わせて、AWS の担当者が AWS 専有インベントリ管理ツールを使用して、AWS ハードウェアの資産に所有者を割り当て、追跡および監視を行っています。AWS の調達およびサプライチェーンチームは、すべての AWS サプライヤとの関係を維持しています。詳細については、ISO 27001 基準の付録 A、ドメイン 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。
	DCS-01.2	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?	
データセンター セキュリティ 統制された アクセス ポイント	DCS-02.1	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、および保安巡回など) は実装されていますか?	物理的セキュリティ統制には、フェンス、壁、保安スタッフ、監視カメラ、侵入検知システム、その他の電子的手段などの境界統制が含まれますが、それに限定されるものではありません。AWS SOC レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。詳細については、ISO 27001 基準の付録 A、ドメイン 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。
データセンター セキュリティ 設備の識別	DCS-03.1	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。
データセンター セキュリティ オフサイトの 承認	DCS-04.1	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?(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、レプリケーションなど)	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、次のウェブサイトです入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。 http://aws.amazon.com/security 。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
データセンター セキュリティ オフサイトの 設備	DCS-05.1	資産管理と設備の用途変更 について規定するポリシー と手続きの証拠となる文書 を、テナントに提供してい ますか?	ISO 27001 基準に合わせて、AWS の処理手順には、ストレージデバイスが製品寿命 に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセ スが含まれています。AWS は DoD 5220.22-M (国家産業セキュリティプログラム運 営マニュアル) または NIST 800-88 (媒体のサンタイズに関するガイドライン) に詳 述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの 手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準 の慣行に従って、消磁するか、物理的に破壊されます。 詳細については、ISO 27001 基準の付録 A、ドメイン 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。
データセンター セキュリティ ポリシー	DCS-06.1	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、基 準、および手続きが規定さ 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 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 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。
	DCS-06.2	従業員および関係するサード パーティーが文書化され たポリシー、基準、および 手順についてトレーニング を受けたことを示す証拠を 提供できますか?	ISO 27001 基準に合わせて、すべての AWS 従業員は、修了時に承認を必須とする定 期的な情報セキュリティトレーニングを修了しています。従業員が制定されたポリ シーを理解し遵守していることを確認するために、コンプライアンス監査を定期的 に実施しています。詳細については、次のウェブサイトです。入手可能な AWS クラウ ドセキュリティホワイトペーパーを参照してください。 http://aws.amazon.com/security 。 AWS は独立監査人により ISO 27001 認定に準拠している旨の審査と認定を受けてい ます。また、AWS SOC1 および SOC2 レポートにも詳細な情報が記載されています。
データセンター セキュリティ 保護エリアの 承認	DCS-07.1	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?	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。本文書の執筆時点では、リージョンは 11 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)、欧州 (フランクフルト)、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)、中国 (北京)、南米 (サンパウロ) です。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
データセンター セキュリティ 権限のない個人の 入場	DCS-08.1	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?	物理的アクセスは、建物の周辺および入り口において、監視カメラや侵入検知システムなどの電子的手段を用いる専門の保安要員その他の手段により、厳重に管理されています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。サーバー設置箇所への物理アクセスポイントは、AWS データセンター物理セキュリティポリシーの規定により、閉回路テレビ (CCTV) カメラで録画されています。
データセンター セキュリティ ユーザー アクセス	DCS-09.1	ユーザーおよびサポート要員による情報資産および機能への物理的なアクセスを制限していますか?	AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監査中に外部の独立監査人によって確認されます。
暗号化および キー管理 使用権限管理	EKM-01.1	キーを識別可能な所有者にバインディングするキー管理ポリシーがありますか?	AWS では、S3、EBS、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用できるようにしています。VPC セッションも暗号化されます。加えて、お客様は AWS Key Management Systems (KMS) を活用して暗号化キーの作成と管理を行えます (https://aws.amazon.com/kms/ を参照)。 AWS は、AWS インフラストラクチャ内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストに必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認定をセキュリティ保護、配布するために使用されます。 AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。
暗号化および キー管理 キーの生成	EKM-02.1	テナントごとに一意の暗号化キーを作成できる機能がありますか?	AWS では、S3、EBS、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC への IPSec トンネルも暗号化されます。加えて、お客様は AWS Key Management Systems (KMS) を活用して暗号化キーの作成と管理を行えます (https://aws.amazon.com/kms/ を参照)。
	EKM-02.2	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?	KMS の詳細については、AWS SOC レポートを参照してください。
	EKM-02.3	キー管理手続きを維持していますか?	加えて、詳細については AWS クラウドセキュリティホワイトペーパー (http://aws.amazon.com/security で入手可能) を参照してください。
	EKM-02.4	暗号化キーのライフサイクルの各ステージで、所有権を文書化していますか?	AWS は、AWS インフラストラクチャ内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。AWS は NIST で承認されたキー管理テクノロジーとプロセスを AWS 情報システムで使用して対称暗号化キーを作成、管理、配布しています。
	EKM-02.5	暗号化キーを管理するためにサードパーティー/オープンソース/専用フレームワークを活用していますか?	対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストに必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認定をセキュリティ保護、配布するために使用されます。 AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
暗号化および キー管理 暗号化	EKM-03.1	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、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC への IPSec トンネルも暗号化されます。加えて、お客様は AWS Key Management Systems (KMS) を活用して暗号化キーの作成と管理を行えます (https://aws.amazon.com/kms/ を参照)。
	EKM-03.2	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?	KMS の詳細については、AWS SOC レポートを参照してください。 加えて、詳細については AWS クラウドセキュリティホワイトペーパー (http://aws.amazon.com/security で入手可能) を参照してください。
	EKM-03.3	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 (たとえば、ID ベースの暗号化)?	
	EKM-03.4	暗号化管理のポリシー、手順、およびガイドラインを確立および定義しているドキュメントはありますか?	
暗号化および キー管理 ストレージ および アクセス	EKM-04.1	オープン/検証済みフォーマットおよび標準アルゴリズムを使用する、プラットフォームおよびデータに適した暗号化がありますか?	AWS では、S3、EBS、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。加えて、お客様は AWS Key Management Systems (KMS) を活用して暗号化キーの作成と管理を行えます (https://aws.amazon.com/kms/ を参照)。KMS の詳細については、AWS SOC レポートを参照してください。
	EKM-04.2	暗号化キーはクラウド利用者または信頼できるキー管理プロバイダーによって維持されていますか?	AWS は、AWS インフラストラクチャ内で採用される必要な暗号化用の暗号キーを確立、管理しています。AWS は NIST で承認されたキー管理テクノロジーとプロセスを AWS 情報システムで使用して対称暗号キーを作成、管理、配布しています。
	EKM-04.3	暗号化キーをクラウドに保管していますか?	対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストに必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認定をセキュリティ保護、配布するために使用されます。
	EKM-04.4	キー管理とキー使用の責任は分離されていますか?	AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
ガバナンス および リスク管理 基礎の要件	GRM-01.1	インフラストラクチャのすべてのコンポーネント(ハイパーバイザー、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 基準の付録 A、ドメイン 14 および 18 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。
	GRM-01.2	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?	
	GRM-01.3	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?	
ガバナンス および リスク管理 リスク評価	GRM-02.1	テナントが業界標準の連続モニタリングを実装できるように、セキュリティ統制ヘルスデータを提供していますか(連続モニタリングによって、物理的および論理的統制ステータスの連続的なテナントの検証が可能になりますか)?	AWS は、独立監査人のレポートと認定を発行して、AWS が規定し、運用しているポリシー、プロセス、および統制に関する大量の情報をお客様に提供しています。関連する認定とレポートを AWS のお客様に提供できます。論理的統制の連続モニタリングは、お客様がお客様のシステムで実行できます。
	GRM-02.2	データガバナンス要件に関連したリスク評価を少なくとも年に1回は行っていますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
ガバナンス および リスク管理 管理の監視	GRM-03.1	お客様の技術、ビジネス、および経営管理者は、管理者および従業員の責任範囲に関して、自分自身および従業員の両方のセキュリティポリシー、手続き、および基準の意識およびコンプライアンスを維持する責任を負っていますか？	Amazon の統制環境は、当社の最上層部で開始されます。役員とシニアリーダーは、当社のカラーと中心的な価値を規定する際、重要な役割を担っています。各従業員には当社の業務行動倫理規定が配布され、定期的なトレーニングを受けます。作成したポリシーを従業員が理解し、従うために、コンプライアンス監査が実施されます。詳細については、AWS リスクとコンプライアンスホワイトペーパー (http://aws.amazon.com/compliance) を参照してください。
ガバナンス および リスク管理 管理プログラム	GRM-04.1	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 はお客様に ISO 27001 認定を提供しています。ISO 27001 認定は特に AWS ISMS に焦点を合わせており、AWS の内部プロセスがどのように ISO 基準に従っているかを測定します。認定とは、サードパーティーによる承認を受けた独立監査機関が AWS のプロセスおよびコントロールを評価し、ISO 27001 認定基準に沿って運用されていることを検証したことを意味します。詳細については、AWS Compliance ISO 27001 FAQ ウェブサイトを参照してください。 http://aws.amazon.com/compliance/iso-27001-faqs/ 。
	GRM-04.2	自社の情報セキュリティ管理プログラム (Information Security Management Program/ISMP) を少なくとも年に 1 回は確認しますか？	
ガバナンス および リスク管理 管理のサポートおよび かかわり	GRM-05.1	プロバイダー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していることを確認していますか？	AWS は、情報および関連技術のための統制目標 (COBIT) フレームワークに基づいて情報セキュリティフレームワークとポリシーを制定していて、ISO 27002 統制、米国公認会計士協会 (AICPA) の信頼提供の原則 (Trust Services Principles)、PCI DSS 3.1 版、および米国国立標準技術研究所 (NIST) 出版物 800-53 改訂 3 (連邦情報システム向けの推奨セキュリティ管理) に基づいて ISO 27001 認定可能なフレームワークを実質的に統合しています。
ガバナンス および リスク管理 ポリシー	GRM-06.1	情報セキュリティおよびプライバシーポリシーは、業界基準 (ISO-27001、ISO-22307、CoBIT など) に準拠していますか？	AWS は、ISO 27001 基準に合わせてサードパーティーとの関係を管理しています。
	GRM-06.2	プロバイダー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？	AWS サードパーティーの要件は、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監査中に外部の独立監査人によって確認されます。
	GRM-06.3	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？	AWS コンプライアンスプログラムに関する情報は、 http://aws.amazon.com/compliance/ のウェブサイトにて一般公開されています。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	GRM-06.4	準拠しているコントロール、基準、認定、および/または規制を開示していますか?	
ガバナンス および リスク管理 ポリシーの実施	GRM-07.1	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および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、次のウェブサイトですぐ入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。 http://aws.amazon.com/security 。詳細については、ISO 27001 基準の付録 A、ドメイン 7 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。
	GRM-07.2	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?	
ガバナンス および リスク管理 ビジネスおよびポリシー変更の影響	GRM-08.1	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 を参照してください。AWS は独立監査人により ISO 27001 認定に準拠している旨の審査と認定を受けています。
ガバナンス および リスク管理 ポリシーの レビュー	GRM-09.1	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?	AWS クラウドセキュリティホワイトペーパーおよび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 および http://aws.amazon.com/compliance で入手可能) 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。
	GRM-09.2	プライバシーおよびセキュリティポリシーのレビューを最低でも毎年実施していますか?	プライバシーおよびセキュリティポリシーのレビューの詳細については、AWS SOC レポートを参照してください。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
ガバナンス および リスク管理 評価	GRM-10.1	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？	<p>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。</p> <p>AWS は独立監査人により ISO 27001 認定に準拠している旨の審査と認定を受けています。</p> <p>AWS のリスク管理フレームワークの詳細については、AWS リスクとコンプライアンスホワイトペーパー (aws.amazon.com/security) を参照してください。</p>
	GRM-10.2	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 (たとえば、監査結果、脅威と脆弱性の分析、規制への準拠など)?	
ガバナンス および リスク管理 プログラム	GRM-11.1	リスクを管理するための文書化された組織全体のプログラムがありますか？	<p>AWS は、ISO 27001 に合わせて、リスク管理プログラムを維持してリスクを軽減し、管理しています。</p> <p>AWS マネジメントには、リスクを緩和または管理するためのリスク特定やコントロールの実装など、戦略的事業計画があります。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。</p> <p>AWS のリスク管理プログラムは、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監査中に外部の独立監査人によって確認されます。</p>
	GRM-11.2	組織全体のリスク管理プログラムのドキュメントを入手可能にしていますか？	
ヒューマン リソース 資産の返却	HRS-01.1	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？	<p>AWS のお客様は、プライバシー違反についてお客様の環境を監視する責任を有します。</p> <p>AWS SOC 1 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。</p>
	HRS-01.2	プライバシーポリシーは、業界基準に合わせていますか？	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
ヒューマン リソース 経歴の審査	HRS-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、および関連するサードパーティーは、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。 AWS SOC レポートには、経歴検証のために実施している統制の詳細が記載されています。
ヒューマン リソース 雇用契約	HRS-03.1	従業員の特定の役割および実行する必要のある情報セキュリティ統制に関して、従業員を特別にトレーニングしていますか？	ISO 27001 基準に合わせて、すべての AWS 従業員は、修了時に承認を必須とする定期的な役割に基づく AWS セキュリティトレーニングを修了しています。従業員が制定されたポリシーを理解し遵守していることを確認するために、コンプライアンス監査を定期的実施しています。詳細については、SOC レポートを参照してください。 AWS システムとデバイスをサポートするすべての従業員は、アクセス権を付与される前に機密保持契約書に署名します。さらに、採用の際には、利用規定および Amazon 業務行動倫理規定 (行動規定) ポリシーを読んで同意することが従業員に求められます。
	HRS-03.2	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？	
	HRS-03.3	すべての従業員は、お客様およびテナントの情報を保護するための条件として、NDA または守秘契約に署名することが求められていますか？	
	HRS-03.4	機密システムへのアクセスを取得および維持には、トレーニングプログラムを期限内に正常に完了することが前提条件と見なされていますか？	
	HRS-03.5	従業員に少なくとも年に 1 回は認識プログラムのトレーニングを提供していますか？	
ヒューマン リソース 雇用終了	HRS-04.1	雇用の変更または終了を管理するための文書化されたポリシー、手順、およびガイドラインが設けられていますか？	AWS の人事チームは、従業員およびベンダーの終了および役職の変更のために従う必要がある内部管理責任を定義しています。 AWS SOC レポートには、詳細情報が記載されています。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	HRS-04.2	前述の手順およびガイドラインでは、タイムリーなアクセスの失効と資産の返却に対応していますか？	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 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 セキュリティプロセスの概要ホワイトペーパーの「従業員のライフサイクル」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 7 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。
ヒューマン リソース 携帯デバイス および モバイル デバイス	HRS-05.1	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およびテナント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（プロバイダー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。	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。お客様には、モバイルセキュリティデバイスおよびお客様のコンテンツへのアクセスを管理する責任があります。
ヒューマン リソース 機密保持契約	HRS-06.1	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。
ヒューマン リソース ロールおよび 責任	HRS-07.1	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 クラウドセキュリティホワイトペーパーおよび AWS リスクとコンプライアンスホワイトペーパーを参照してください。これらのホワイトペーパーは次のウェブサイトで見ることができます。 http://aws.amazon.com/security および http://aws.amazon.com/compliance 。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
ヒューマン リソース 利用規定	HRS-08.1	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 には、毎年 (またはポリシーに影響するシステムへの大きな変更が発生したときに) 確認、更新される正式なアクセスコントロールポリシーがあります。このポリシーでは、目的、範囲、役割、責任、および管理コミットメントについて取り上げています。AWS は最小権限という概念を導入しており、ユーザーがジョブ機能を実行するために必要最小限のアクセスを許可しています。
	HRS-08.2	調査テクノロジー (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?	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。お客様には、モバイルセキュリティデバイスおよびお客様のコンテンツへのアクセスを管理する責任があります。
	HRS-08.3	調査テクノロジー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?	詳細情報については、ISO 27001 基準および 27018 行動規範を参照してください。AWS は独立監査人により ISO 27001 および ISO 27018 に準拠している旨の審査と認定を受けています。
ヒューマン リソース トレーニング および意識	HRS-09.1	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) に関する役割に基づいた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していますか?	ISO 27001 基準に合わせて、すべての AWS 従業員は、修了時に承認を必須とする定期的な情報セキュリティトレーニングを修了しています。従業員が制定されたポリシーを理解し遵守していることを確認するために、コンプライアンス監査を定期的に行っています。 AWS の役割と責任は、SOC、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監査中に外部の独立監査人によって確認されます。
	HRS-09.2	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、適切な教育を受けていますか?	
ヒューマン リソース ユーザーの責任	HRS-10.1	公開されているセキュリティポリシー、手続き、基準、適用可能な規制の要件に対する意識と準拠を維持するために、ユーザーに自身の責任について意識させていますか?	AWS は、様々な方法でグローバルレベルの内部コミュニケーションを実施することで、従業員が各自の役割と責任を理解することを手助けし、重要なイベントについて適時伝達しています。この方法には、新規に雇用した従業員に対するオリエンテーションおよびトレーニングプログラムや、Amazon イン트라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 基準の付録 A、ドメイン 7 および 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。さら
	HRS-10.2	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?	に、詳細については、AWS クラウドセキュリティホワイトペーパー (http://aws.amazon.com/security) を参照してください。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	HRS-10.3	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?	
ヒューマン リソース ワークスペース	HRS-11.1	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 および 9 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 レポートには、AWS リソースに対する不正アクセスを防ぐために AWS が実行する特定の統制行動について、その他の詳細情報が記載されています。
	HRS-11.2	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?	AWS は AWS システム内でシステムとデバイス間で監査可能なイベントカテゴリを識別しています。サービスチームは監査機能を設定して、要件に従って継続的にセキュリティ関連イベントを記録しています。監査記録には、必要な分析要件をサポートするために、データ要素のセットが含まれます。さらに AWS セキュリティチームまたはその他の適切なチームは、要求時に検査または分析を実行するため、またはセキュリティ関連のイベントやビジネスに影響するイベントに応じて、監査記録を使用できます。
	HRS-11.3	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?	
アイデンティティ および アクセス管理 管理ツールの アクセス	IAM-01.1	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? (ハイパーバイザー、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 は、ISO 27001 基準に合わせて、AWS リソースに対する論理アクセスについて最小限の基準を示す正規のポリシー、手続きを規定しています。AWS SOC レポートには、AWS リソースに対するアクセスプロビジョニングを管理するために用意されている統制の概要が記載されています。 詳細については、次のウェブサイトですぐ入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。 http://aws.amazon.com/security 。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	IAM-01.2	情報セキュリティ管理システムへの特権アクセス(管理者レベル)を監視およびログしていますか?	<p>AWS は AWS システム内でシステムとデバイス間で監査可能なイベントカテゴリを識別しています。サービスチームは監査機能を設定して、要件に従って継続的にセキュリティ関連イベントを記録しています。ログストレージシステムは、ログストレージの次のニーズが発生すると自動的に容量を増やす、スケーラブルで高可用性のサービスを提供するように設計されています。監査記録には、必要な分析要件をサポートするために、データ要素のセットが含まれます。さらに AWS セキュリティチームまたはその他の適切なチームは、要求時に検査または分析を実行するため、またはセキュリティ関連のイベントやビジネスに影響するイベントに応じて、監査記録を使用できます。</p> <p>AWS チームの指定された関係者は、監査処理が失敗した場合に、自動化されたアラートを受け取ります。監査処理の失敗には、ソフトウェア/ハードウェアのエラーなどが含まれます。オンコール担当者は、アラートを受け取るとトラブルチケットを発行し、解決されるまでイベントを追跡します。</p> <p>AWS のログおよびモニタリングプロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP コンプライアンスへの AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。</p>
アイデンティティ および アクセス管理 ユーザー アクセス ポリシー	IAM-02.1	ビジネスの目的に必要な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?	<p>AWS SOC 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 セキュリティプロセスの概要ホワイトペーパーの「従業員のライフサイクル」を参照してください。</p> <p>詳細については、ISO 27001 基準の付録 A、ドメイン 9 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。</p>
	IAM-02.2	ビジネスの目的で不要になったシステムアクセス権を削除できる速度を追跡するメトリックスを用意していますか?	
アイデンティティ および アクセス管理 診断および 設置ポートの アクセス アクセス	IAM-03.1	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?	<p>所定の統制によってシステムおよびデータのアクセスを制限し、AWS アクセスポリシーに従ってシステムまたはデータに対するアクセスを制限および監視できるようにしています。さらに、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様とは論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC、ISO 27001、PCI、ITAR、および FedRAMP の監査中に独立監査人によって確認されます。</p>
アイデンティティ および アクセス管理 ポリシーと手順	IAM-04.1	IT インフラストラクチャにアクセス可能なすべての従業員のアイデンティティを、アクセスレベルも含めて管理および保存していますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	IAM-04.2	ネットワークにアクセス可能なすべての従業員のユーザーアイデンティティを、アクセスレベルも含めて管理および保存していますか?	
アイデンティティおよびアクセス管理 役割分担	IAM-05.1	クラウドサービス内で役割分担を維持する方法に関する文書を、テナントに提供していますか?	お客様は、AWS リソースの役割分担を管理することができます。 AWS 社内では ISO 27001 基準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 6.1 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。
アイデンティティおよびアクセス管理 ソースコードのアクセス制限	IAM-06.1	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、権限を持つ担当者のみアクセスを制限していますか?	AWS は、ISO 27001 基準に合わせて、AWS リソースに対する論理アクセスについて最小限の基準を示す正規のポリシー、手続きを規定しています。AWS SOC レポートには、AWS リソースに対するアクセスプロビジョニングを管理するために用意されている統制の概要が記載されています。 詳細については、AWS セキュリティプロセスの概要 (http://aws.amazon.com/security で入手可能) を参照してください。
	IAM-06.2	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、権限を持つ担当者のみアクセスを制限していますか?	
アイデンティティおよびアクセス管理 サードパーティーのアクセス	IAM-07.1	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ゾーンは、独立した障害ゾーンとして設計されています。障害時には、自動プロセスが、顧客データを影響を受けるエリアから移動します。AWS SOC レポートに詳細情報が記載されています。ISO 27001 基準の付録 A、ドメイン 15 に詳細が記載されています。AWS は独立監査人により ISO 27001 認定に準拠している旨の審査と認定を受けています。
	IAM-07.2	プロバイダー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ーを使用してサービスの継続性を監視していますか?	
	IAM-07.3	依存しているサービスごとに、複数のプロバイダーがありますか?	
	IAM-07.4	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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	IAM-07.5	災害を宣言する機能をテナントに提供していますか?	
	IAM-07.6	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?	
	IAM-07.7	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?	
アイデンティティおよびアクセス管理 ユーザー アクセスの制限 および承認	IAM-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。所定の統制によってシステムおよびデータのアクセスを制限し、システムまたはデータに対するアクセスを制限および監視できるようにしています。さらに、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様とは論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC、ISO 27001、PCI、ITAR、および FedRAMP の監査中に独立監査人によって確認されます。
	IAM-08.2	アクセス制御目的のためのプロバイダー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?	
アイデンティティおよびアクセス管理 ユーザー アクセスの承認	IAM-09.1	マネジメントは、ユーザー（従業員、請負業者、お客様（テナント）、ビジネスパートナー、サプライヤーなど）がデータおよび所有/管理する（物理または仮想）アプリケーション、インフラストラクチャシステム、およびネットワークコンポーネントにアクセスする前に、ユーザーアクセスの承認と制限をプロビジョンしていますか?	AWS 人事管理システムのオンボーディングワークフロープロセスの一環として、一意のユーザー ID が作成されます。デバイスプロビジョニングプロセスは、デバイスの ID を確実に一意にするうえで役立ちます。両方のプロセスとも、ユーザーアカウントまたはデバイスを確立するためのマネージャーの承認が含まれます。最初の認証は、プロビジョニングプロセスの一部としてユーザーに対面で提供されるとともに、デバイスにも提供されます。内部ユーザーは SSH パブリックキーをアカウントに関連付けることができます。システムアカウントの認証は、リクエストの ID を確認した後で、アカウント作成プロセスの一部としてリクエストに提供されます。
	IAM-09.2	申請があった場合、ユーザー（従業員、請負業者、お客様（テナント）、ビジネスパートナー、サプライヤーなど）がデータおよび所有/管理する（物理または仮想）アプリケーション、インフラストラクチャシステム、およびネットワークコンポーネントにアクセスできるようにしますか?	AWS は、内部者による不適切なアクセスの脅威に対処するための統制を提供しています。すべての認定とサードパーティーによる証明で、論理アクセスの予防統制と検出統制が評価されています。さらに、定期的なリスク評価時に、内部者によるアクセスの統制および監視方法を評価しています。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
アイデンティティ および アクセス管理 ユーザー アクセスの レビュー	IAM-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定期的に確認されており、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 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 レポートに記載されています。
	IAM-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?	詳細については、ISO 27001 基準の付録 A、ドメイン 9 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。
	IAM-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?	
IAM-11.1	従業員、請負業者、顧客、ビジネスパートナー、または関係するサードパーティー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 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 セキュリティプロセスの概要ホワイトペーパーの「従業員のライフサイクル」を参照してください。 詳細については、ISO 27001 基準の付録 A、ドメイン 9 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。	
アイデンティティ および アクセス管理 ユーザー アクセスの失効	IAM-11.2	ユーザーアクセスの状況の変化には、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?	
	IAM-12.1	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。 AWS Identity and Access Management (IAM) は AWS マネジメントコンソールまたは AWS API への委任アクセスに対する ID フェデレーションをサポートしています。ID フェデレーションを利用すれば、IAM ユーザーを作成しなくても、AWS アカウントのリソースに対する安全なアクセス権が外部の ID (フェデレーティッドユーザー) に付与されます。これらの外部 ID は、企業 ID プロバイダー (Microsoft Active Directory や AWS Directory Service など) またはウェブ ID プロバイダー (Amazon Cognito、Login with Amazon、Facebook、Google、または任意の OpenID Connect (OIDC) 互換プロバイダーなど) を経由することができます。
アイデンティティ および アクセス管理 ユーザー ID 認証情報	IAM-12.1	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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	IAM-12.2	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?	
	IAM-12.3	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?	
	IAM-12.4	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 (例: XACML など) がありますか?	
	IAM-12.5	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?	
	IAM-12.6	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?	
	IAM-12.7	サードパーティーの 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?	
	IAM-12.8	パスワード (最低文字数、使 用期間、履歴、複雑さ) およ びアカウントロックアウト (ロックアウトしきい値、 ロックアウト期間) ポリシー の実施をサポートしていま すか?	AWS Identity and Access Management (IAM) により、お客様はユーザーの AWS サービスおよびリソースへのアクセスを安全にコントロールすることができます。IAM の詳細については、 https://aws.amazon.com/iam/ のウェブサイトを参照してください。AWS SOC 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。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	IAM-12.9	テナントおよびお客様がアカウントでパスワードおよびアカウントロックアウトのポリシーを定義するのを許可していますか?	
	IAM-12.10	最初のログオンでパスワードの変更を強制する機能をサポートしていますか?	
	IAM-12.11	ロックアウトしたアカウントのロック解除を行うメカニズム(メールによるセルフサービス、定義済みの秘密の質問、手動のロック解除など)を設けていますか?	
アイデンティティおよびアクセス管理 ユーティリティ プログラムの アクセス	IAM-13.1	仮想化パーティションの重要な機能(シャットダウン、クローンなど)を管理できるユーティリティは、適切に制限および監視されていますか?	ISO 27001 基準に合わせて、システムユーティリティは適切に制限および監視されています。AWS SOC レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。 詳細については、AWS セキュリティプロセスの概要 (http://aws.amazon.com/security で入手可能) を参照してください。
	IAM-13.2	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?	
	IAM-13.3	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?	
インフラストラクチャおよび仮想化セキュリティ 監査記録および侵入検知	IVS-01.1	適時の検出、根本原因の分析ごとの調査、および事故対応を容易にするために、ファイルの完全性(ホスト)およびネットワークの侵入検出(IDS)ツールは実装されていますか?	AWS 事故対応プログラム(事故の検出、調査、および対応)は、ISO 27001 基準に合わせて開発されており、システムユーティリティは適切に制限および監視されています。AWS SOC 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 セキュリティプロセスの概要 (http://aws.amazon.com/security で入手可能) を参照してください。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	IVS-01.2	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?	
	IVS-01.3	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?	
	IVS-01.4	監査記録は一元的に保管および維持されていますか?	
	IVS-01.5	監査記録はセキュリティイベントのために (自動化ツールなどで) 定期的にレビューされていますか?	<p>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。</p> <p>AWS は、自動モニタリングシステムを活用して、ハイレベルなサービスパフォーマンスと可用性を提供します。内部的、外部的両方の使用において、様々なオンラインツールを用いた積極的モニタリングが可能です。AWS 内のシステムには膨大な装置が備わっており、主要なオペレーションメトリックをモニタリングしています。重要計測値が早期警戒しきい値を超える場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。オンコールスケジュールが採用されているので、担当者が運用上の問題にいつでも対応できます。ポケットベルシステムがサポートされ、アラームが迅速かつ確実に運用担当者に届きます。</p> <p>詳細については、次のウェブサイトですぐ入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。 http://aws.amazon.com/security。</p>
インフラストラクチャおよび仮想化セキュリティ変更検知	IVS-02.1	運用状況 (停止、オフ、運用中など) に関係なく、仮想マシンのイメージに対する変更を記録し、アラートで通知していますか?	仮想マシンは、EC2 サービスの一部としてお客様に割り当てられています。お客様は、使用されるリソースとリソースの場所に関する統制を有しています。詳細については、AWS のウェブサイト (http://aws.amazon.com) を参照してください。
	IVS-02.2	仮想マシンに対する変更、またはイメージの移動とその後のイメージ整合性の検証は、電子的な方法 (ポータルやアラートなど) によってお客様に即座に提供されていますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
インフラストラクチャおよび仮想化セキュリティ 時計の同期	IVS-03.1	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。
インフラストラクチャおよび仮想化セキュリティ 容量およびリソース計画	IVS-04.1	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 サービスの制限の詳細および特定のサービスの制限の増加をリクエストする方法については、 http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html にある AWS のウェブサイトを参照してください。 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。
	IVS-04.2	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?	
	IVS-04.3	システム容量の要件では、テナントにサービスを提供するために使用されるすべてのシステムの現在の容量、計画されている容量、および予測される容量の必要を考慮に入れていますか?	
	IVS-04.4	テナントにサービスを提供するために使用されるすべてのシステムで、規制、契約、およびビジネス上の要件を満たすために、システムパフォーマンスが継続的に監視および調整されていますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
インフラストラクチャおよび仮想化セキュリティ管理 - 脆弱性の管理	IVS-05.1	セキュリティの脆弱性評価ツールおよびサービスは、使用されている仮想化技術(仮想化の認識など)に対応していますか?	<p>現在、Amazon EC2 は、高度にカスタマイズされたバージョンの Xen ハイパーバイザーを利用しています。ハイパーバイザーは、社内および社外の侵害対策チームによって新規および既存の脆弱性と攻撃進路を定期的に評価しています。また、ゲスト仮想マシン間の強力な隔離を維持するためにも適しています。AWS Xen ハイパーバイザーのセキュリティは、評価および監査の際に独立監査人によって定期的に評価されています。</p> <p>AWS 環境内のホストオペレーティングシステム、ウェブアプリケーション、およびデータベースでさまざまなツールを利用した、定期的な内外部の脆弱性のスキャンが実行されます。脆弱性のスキャンと解決手法は、AWS の PCI DSS および FedRAMP への継続的な準拠の一環として定期的に確認されます。</p>
インフラストラクチャおよび仮想化セキュリティネットワークセキュリティ	IVS-06.1	IaaS の提供について、仮想化ソリューションを使用して、階層化セキュリティアーキテクチャ相当のものを作成する方法のガイダンスを顧客に提供していますか?	AWS のウェブサイトでは、AWS の公開ウェブサイト (http://aws.amazon.com/documentation/) で入手できる複数のホワイトペーパーで、階層化セキュリティアーキテクチャ作成のガイダンスを提供しています。
	IVS-06.2	セキュリティドメインおよびゾーン間のデータフローを含むネットワークアーキテクチャダイアグラムを定期的に更新していますか?	<p>境界保護デバイスは、ルールセット、アクセスコントロールリスト (ACL)、および設定を使用してネットワークファブリック間で情報の流れを強制する境界保護デバイスを拒否する deny-all モードで設定されます。</p> <p>Amazon には複数のネットワークファブリックが存在し、それぞれはファブリック間の情報の流れを制御するデバイスによって分離されています。ファブリック間の情報の流れは、それらのデバイスにあるアクセスコントロールリスト (ACL) として存在する承認された機関によって確立されます。これらのデバイスは、ACL の要求に従ってファブリック間の情報の流れを制御します。ACL は適切な従業員が定義、承認し、AWS ACL 管理ツールを使用して管理、デプロイされます。</p>
	IVS-06.3	ネットワーク内のセキュリティドメインおよびゾーン間で許可されたアクセスおよび接続性(ファイアウォールルールなど)に関して、適性を定期的にレビューしていますか?	Amazon の情報セキュリティチームがこれらの ACL を承認します。ネットワークファブリック間の承認されたファイアウォールルールセットとアクセスコントロールリストが、情報の流れを特定の情報システムサービスに制限します。アクセスコントロールリストとルールセットは確認、承認され、定期的に (少なくとも 24 時間ごと) 境界保護デバイスに自動的にプッシュされて、ルールセットとアクセスコントロールリストが最新であることが確認されます。
IVS-06.4	すべてのファイアウォールアクセスコントロールリストはビジネス上の正当性ととも文書化されていますか?		

統制グループ	CID	コンセンサス評価の質問	AWS の回答
インフラストラクチャおよび仮想化セキュリティ OS のセキュリティ強化とベースコントロール	IVS-07.1	ベースラインビルドスタンダードまたはテンプレートの一環として技術的統制(ウイルス対策、ファイル整合性の監視と記録など)を使用して、オペレーティングシステムのセキュリティ強化を行い、ビジネスニーズを満たすのに必要なポート、プロトコル、サービスだけを提供していますか?	<p>AWS ネットワーク管理は、SOC、PCI DSS、ISO 27001、および FedRAMPsm への AWS の継続的な準拠の一環として、第三者の独立監査人によって定期的に確認されます。</p> <p>AWS は、そのインフラストラクチャコンポーネントを通じて最小権限を実装しています。また、特定のビジネス目的を持っていないすべてのポートとプロトコルを禁止しています。AWS は、デバイスの使用に不可欠な機能のみの最小実装という厳格な手法に従っています。ネットワークスキャンを実行し、不要なポートまたはプロトコルが使用されている場合は修正されます。</p> <p>AWS 環境内のホストオペレーティングシステム、ウェブアプリケーション、およびデータベースでさまざまなツールを利用した、定期的な内外部の脆弱性のスキャンが実行されます。脆弱性のスキャンと解決手法は、AWS の PCI DSS および FedRAMP への継続的な準拠の一環として定期的に確認されます。</p>
インフラストラクチャおよび仮想化セキュリティ 運用環境および非運用環境	IVS-08.1	SaaS または PaaS の提供について、運用プロセスとテストプロセスで別の環境をテナントに提供していますか?	AWS のお客様は、運用環境とテスト環境を作成および保持する機能と責任を有します。AWS のウェブサイトでは、AWS サービスを利用して環境を作成する場合のガイダンスを提供しています (http://aws.amazon.com/documentation/)。
	IVS-08.2	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?	
	IVS-08.3	運用環境および非運用環境を論理的および物理的に分離していますか?	
インフラストラクチャおよび仮想化セキュリティ セグメント化	IVS-09.1	ビジネスおよびお客様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ファイアウォールまたは仮想ファイアウォールによって保護されていますか?	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 13 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。
	IVS-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ファイアウォールまたは仮想ファイアウォールによって保護されていますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	IVS-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ファイアウォールまたは仮想ファイアウォールによって保護されていますか?	
	IVS-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ファイアウォールまたは仮想ファイアウォールによって保護されていますか?	
インフラストラクチャおよび仮想化セキュリティ VM セキュリティ - vMotion データ保護	IVS-10.1	物理的なサーバー、アプリケーション、またはデータを仮想サーバーに移行する際、セキュアまたは暗号化された通信チャネルを使用していますか?	AWS では、S3、EBS、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用できるようにしています。VPC セッションも暗号化されます。
	IVS-10.2	物理的なサーバー、アプリケーション、またはデータを仮想サーバーに移行する際、本稼働レベルのネットワークから分離されたネットワークを使用していますか?	AWS のお客様は、お客様のデータの統制と所有権を有しています。AWS は、お客様が運用環境および非運用環境を保守および開発できるようにしています。運用データが非運用環境にレプリケートされないようにするのは、お客様の責任です。
インフラストラクチャおよび仮想化セキュリティ VMM セキュリティ - ハイパーバイザのセキュリティ強化	IVS-11.1	仮想システムをホストするシステムにおいて、技術的統制 (2 要素認証、監査証跡、IP アドレスフィルタリング、ファイアウォール、管理コンソールへの TLS カプセル化された通信など) のサポートにより、最小権限の原則に基づいて、すべてのハイパーバイザー管理機能または管理コンソールへの個人アクセスを制限していますか?	AWS は最小権限という概念を導入しており、ユーザーがジョブ機能を実行するために必要最小限のアクセスを許可しています。ユーザーアカウントの作成では、最小アクセス権を持つユーザーアカウントが作成されます。これらの最小権限を超えるアクセスには、適切な認証が必要になります。アクセスコントロールの詳細については、AWS SOC レポートを参照してください。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
インフラストラクチャおよび仮想化セキュリティ ワイヤレスのセキュリティ	IVS-12.1	ワイヤレスネットワーク環境の境界を保護するためにポリシーと手続きが規定され、メカニズムが構成および実装され、不正なワイヤレストラフィックを制限するように設定されていますか？	AWS ネットワーク環境を保護するためのポリシー、手続き、およびメカニズムが用意されています。 AWS セキュリティ統制は、SOC、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監査中に外部の独立監査人によって確認されます。
	IVS-12.2	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ワイヤレス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)?	
	IVS-12.3	ワイヤレス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？	
インフラストラクチャおよび仮想化セキュリティ ネットワークアーキテクチャ	IVS-13.1	ネットワークアーキテクチャダイアグラムでは、法的コンプライアンスに影響を及ぼしかねない高リスクの環境やデータフローを明確に特定していますか？	AWS のお客様は、お客様が定義した要件に従って、お客様のネットワークセグメントを管理する責任を有します。 AWS 内部では、AWS のネットワークセグメントは ISO 27001 基準に合わせて作成されています。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。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	IVS-13.2	異常な送受信トラフィックパターン (MAC スプーフィングや ARP ポイズニング攻撃など) および/または分散サービス妨害 (DDoS) 攻撃に関連したネットワークベースの攻撃の検出とタイムリーな応答のために、技術的な措置を導入して、深層防御技術 (ディープパケット分析、トラフィックスロットリング、ブラックホーリングなど) を適用していますか?	<p>AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします (お客様のインスタンスはこのスキャンの対象外です)。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、脆弱性に対する外部からの脅威の査定が、独立系のセキュリティ会社によって定期的に行われます。これらの査定に起因する発見や推奨事項は、分類整理されて AWS 上層部に報告されます。</p> <p>さらに、AWS 統制環境は、通常の内部的および外部的リスク評価によって規定されています。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。</p> <p>AWS セキュリティ統制は、SOC、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監査中に外部の独立監査人によって確認されます。</p>
相互運用性 および ポータビリティ API	IPY-01	サービスで利用可能なすべての API のリストを公開して、どれが標準でどれがカスタマイズされたものかを示していますか?	<p>AWS API の詳細については、https://aws.amazon.com/documentation/ にある AWS ウェブサイトをご覧ください。</p> <p>AWS は、ISO 27001 基準に合わせて、AWS リソースに対する論理アクセスについて最小限の基準を示す正規のポリシー、手続きを規定しています。AWS SOC レポートには、AWS リソースに対するアクセスプロビジョニングを管理するために用意されている統制の概要が記載されています。</p> <p>詳細については、次のウェブサイトで入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。http://aws.amazon.com/security。</p>
相互運用性 および ポータビリティ データ リクエスト	IPY-02	非構造化された顧客データは、リクエストに応じて業界標準の形式 (.doc、.xls、または .pdf) で入手可能ですか?	
相互運用性 および ポータビリティ ポリシーおよび 法務	IPY-03.1	お客様のサービスとサードパーティー製アプリケーションとの間の相互運用性に関して API の使用について規定するポリシーおよび手順 (サービスレベルアグリーメントなど) を提供していますか?	
	IPY-03.2	お客様のサービスで送受信するアプリケーションデータの移行について規定するポリシーおよび手順 (サービスレベルアグリーメントなど) を提供していますか?	<p>お客様は、お客様のコンテンツの統制と所有権を維持します。お客様は、AWS プラットフォーム内外の両方におけるアプリケーションおよびコンテンツの移行方法を独自の裁量に基づいて選択できます。</p>

統制グループ	CID	コンセンサス評価の質問	AWS の回答
相互運用性 および ポータビリティ 標準化された ネットワーク プロトコル	IPY-04.1	データのインポート、データのエクスポート、およびサービスの管理を、安全で（クリアテキストではなく、認証済みなど）、業界で受け入れられた、標準化されたネットワークプロトコルで実行できますか？	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。ストレージオプションの詳細については、 http://aws.amazon.com/choosing-a-cloud-platform を参照してください。
	IPY-04.2	関連する相互運用性およびポータビリティネットワークプロトコル基準の詳細について記載した文書を、お客様（テナント）に提供していますか？	
相互運用性 および ポータビリティ 仮想化	IPY-05.1	相互運用性を確保するために、業界で受け入れられた仮想化プラットフォームおよび標準仮想化フォーマット（OVF など）を使用していますか？	現在、Amazon EC2 は、高度にカスタマイズされたバージョンの Xen ハイパーバイザーを利用しています。ハイパーバイザーは、社内および社外の侵害対策チームによって新規および既存の脆弱性と攻撃進路を定期的に評価しています。また、ゲスト仮想マシン間の強力な隔離を維持するためにも適しています。AWS Xen ハイパーバイザーのセキュリティは、評価および監査の際に独立監査人によって定期的に評価されています。詳細については、次のウェブサイトですぐ入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。 http://aws.amazon.com/security 。
	IPY-05.2	使用中のハイパーバイザーに対して行われたカスタム変更を文書化し、お客様のレビュー用にソリューション固有の仮想化フックをすべて提供していますか？	
モバイル セキュリティ マルウェア対策	MOS-01	情報セキュリティ認識トレーニングの一環として、モバイルデバイス固有のマルウェア対策トレーニングを提供していますか？	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。詳細情報については、ISO 27001 基準の付録 A、ドメイン 12 を参照してください。
モバイル セキュリティ アプリケーション ストア	MOS-02	企業データへのアクセスまたは保管、および/または企業システムへのアクセスが可能なモバイルデバイスで許可されるアプリケーションストアのリストを文書化して提供していますか？	AWS は、情報および関連技術のための統制目標（COBIT）フレームワークに基づいて情報セキュリティフレームワークとポリシーを制定していて、ISO 27002 統制、米国公認会計士協会（AICPA）の信頼提供の原則（Trust Services Principles）、PCI DSS 3.1 版、および米国国立標準技術研究所（NIST）出版物 800-53 改訂 3（連邦情報システム向けの推奨セキュリティ管理）に基づいて ISO 27001 認定可能なフレームワークを効果的に統合しています。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
モバイル セキュリティ 許可される アプリケーション	MOS-03	許可されたアプリケーションおよび許可されたアプリケーションストアから来たアプリケーションだけがモバイルデバイスにロードされることを確認するために、ポリシーの実施機能 (XACML など) を設けていますか?	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。お客様には、モバイルセキュリティデバイスおよびお客様のコンテンツへのアクセスを管理する責任があります。
モバイル セキュリティ 個人所有機器で 許可される ソフトウェア	MOS-04	BYOD (個人所有機器) ポリシーおよびトレーニングでは、個人所有機器で使用が許可されているアプリケーションおよびアプリケーションストアを明示していますか?	
モバイル セキュリティ 意識および トレーニング	MOS-05	従業員のトレーニングで、モバイルデバイスおよびモバイルデバイスの許可された使用方法と要件が明確に定義された、文書化したモバイルデバイスポリシーがありますか?	
モバイル セキュリティ クラウドベース サービス	MOS-06	企業のビジネスデータの使用と保管のためにモバイルデバイス経由で使用できる事前承認されたクラウドベースサービスの文書化されたリストがありますか?	
モバイル セキュリティ 互換性	MOS-07	デバイス、オペレーティングシステム、およびアプリケーションの互換性の問題をテストするための文書化されたアプリケーション検証プロセスを設けていますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
モバイル セキュリティ デバイスの利用 資格	MOS-08	BYOD (個人所有機器) のデバイスおよび BYOD の使用に関する利用資格を定義した BYOD ポリシーを設けていますか?	
モバイル セキュリティ デバイスの在庫	MOS-09	企業データの保存とアクセスが可能なすべてのモバイルデバイスの在庫およびデバイスステータス (OS システムやパッチレベル、紛失または廃棄、デバイスの使用者) を保持していますか?	
モバイル セキュリティ デバイスの管理	MOS-10	企業データの保存、伝送、または処理が許可されているすべてのモバイルデバイスに、一元化されたモバイルデバイス管理ソリューションを導入していますか?	
モバイル セキュリティ 暗号化	MOS-11	お客様のモバイルデバイスポリシーでは、すべてのモバイルデバイスについて、デバイス全体または機密情報として指定されたデータに対して技術的統制による暗号化の使用を義務づけていますか?	
モバイル セキュリティ 脱獄および ルート化	MOS-12.1	お客様のモバイルデバイスポリシーでは、モバイルデバイスに組み込まれたセキュリティ統制を回避することを禁止していますか (脱獄やルート化など)?	
	MOS-12.2	組み込まれたセキュリティ統制の回避を阻止するために、デバイスでの検出コントロールや防止コントロール、または一元化されたデバイス管理システムを設けていますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
モバイル セキュリティ 法務	MOS-13.1	お客様の BYOD ポリシーでは、プライバシーに関する期待、および訴訟、電子情報開示、法務のための停止に関する要求事項を明確に定義していますか?	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。お客様には、モバイルセキュリティデバイスおよびお客様のコンテンツへのアクセスを管理する責任があります。
	MOS-13.2	組み込まれたセキュリティ統制の回避を阻止するために、デバイスでの検出コントロールや防止コントロール、または一元化されたデバイス管理システムを設けていますか?	
モバイル セキュリティ 画面ロック	MOS-14	BYOD および企業所有のデバイスで、自動化された画面ロックを技術的統制によって義務化および強制していますか?	
モバイル セキュリティ オペレーティング システム	MOS-15	お客様の企業の変更管理プロセスによって、モバイルデバイスのオペレーティングシステム、パッチレベル、アプリケーションに対するすべての変更を管理していますか?	
モバイル セキュリティ パスワード	MOS-16.1	企業が提供するモバイルデバイスおよび/または BYOD のモバイルデバイスに関してパスワードポリシーを設けていますか?	
	MOS-16.2	技術的統制 (MDM など) によってパスワードポリシーを強制していますか?	
	MOS-16.3	お客様のパスワードポリシーでは、認証要件 (パスワード/PIN の長さなど) をモバイルデバイスによって変更することが禁止されていますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
モバイル セキュリティ ポリシー	MOS-17.1	BYOD ユーザーが、指定された企業データのバックアップを実行することを義務付けるポリシーを設けていますか？	
	MOS-17.2	BYOD ユーザーが未承認のアプリケーションストアを使用することを禁止するポリシーを設けていますか？	
	MOS-17.3	BYOD ユーザーがマルウェア対策ソフトウェア (サポート対象の場合) を使用することを義務付けるポリシーを設けていますか？	
モバイル セキュリティ リモートワイプ	MOS-18.1	企業の承認を得たすべての BYOD デバイスについて、IT はリモートスワイプまたは企業データスワイプを提供していますか？	
	MOS-18.2	企業が支給したすべてのモバイルデバイスについて、IT はリモートスワイプまたは企業データスワイプを提供していますか？	
モバイル セキュリティ セキュリティ パッチ	MOS-19.1	ご使用のモバイルデバイスでは、デバイスのメーカーまたはキャリアが一般提供している最新のセキュリティ関連パッチがインストールされていますか？	
	MOS-19.2	ご使用のモバイルデバイスでは、企業の IT 担当者が最新のセキュリティパッチをダウンロードできるようにリモート検証が許可されていますか？	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
モバイル セキュリティ ユーザー	MOS-20.1	お客様の BYOD ポリシーでは、BYOD 対象デバイスにおいて使用またはアクセスが許可されているシステムおよびサーバーを明示していますか?	
	MOS-20.2	お客様の BYOD ポリシーでは、BYOD 対象デバイスによってアクセスが許可されているユーザーロールを指定していますか?	
セキュリティ事故 管理、電子情報開 示、およびクラウ ドフォレンジック 各機関との関係と 接点の維持	SEF-01.1	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?	<p>AWS は、ISO 27001 基準の要件に従い、業界団体、リスクおよびコンプライアンス組織、地元機関、および規制団体との接点を維持しています。</p> <p>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。</p>
セキュリティ事故 管理、電子情報開 示、およびクラウ ドフォレンジック 障害管理	SEF-02.1	文書化したセキュリティ事故対応計画がありますか?	<p>AWS の事故対応プログラム、計画、および手続きは、ISO 27001 基準に合わせて作成されています。AWS 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。</p> <p>AWS SOC 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。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。</p> <p>詳細については、AWS クラウドセキュリティホワイトペーパー (http://aws.amazon.com/security で入手可能) を参照してください。</p>
	SEF-02.2	カスタマイズしたテナントの要件をセキュリティ事故対応計画に統合していますか?	
	SEF-02.3	セキュリティ事故時の自社とテナントの責任内容を示した役割と責任の文書を発行していますか?	
	SEF-02.4	過去 1 年間にセキュリティ事故対応計画をテストしたことがありますか?	
セキュリティ事故 管理、電子情報開 示、およびクラウ ドフォレンジック 障害のレポート	SEF-03.1	より細かい分析と警告のために、セキュリティ情報およびイベント管理 (security information and event management/SIEM) システムは、データソース (アプリケーションログ、ファイアウォールログ、IDS ログ、物理アクセスログなど) を結合していますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	SEF-03.2	ロギングおよびモニタリングフレームワークでは、特定のテナントに対する事故を分離できますか?	
セキュリティ事故管理、電子情報開示、およびクラウドフォレンジック 事故対応の法的準備	SEF-04.1	事故対応計画は、法的に許容可能な保管の継続性の管理プロセスおよび統制の業界標準に準拠していますか?	
	SEF-04.2	事故対応機能には、法的に許容可能な法医学データ収集技術および分析技術の使用が含まれますか?	
	SEF-04.3	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?	
	SEF-04.4	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?	
セキュリティ事故管理、電子情報開示、およびクラウドフォレンジック 事故対応のメトリックス	SEF-05.1	すべての情報セキュリティ事故の種類、規模、および影響を監視および数値化していますか?	AWS セキュリティメトリックスは、ISO 27001 基準に従って監視および分析されています。詳細については、ISO 27001 基準の付録 A、ドメイン 16 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。
	SEF-05.2	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?	
サプライチェーン管理、透明性、および説明責任 データの品質と完全性	STA-01.1	データ品質エラーとそれに関連したリスクの検査と対応を行い、クラウドサプライチェーンパートナーと協力してそれらを修正していますか?	お客様は、データの品質および AWS サービスの使用によって生じる可能性がある品質エラーに対して統制と所有権を有しています。 データの完全性およびアクセス管理 (最低限のアクセス権限を含む) に関する詳細については、AWS SOC レポートを参照してください。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	STA-01.2	サプライチェーン内のすべての従業員について、責任の適切な分散、役割ベースのアクセス、最低限のアクセス権限を通じてデータセキュリティリスクを緩和および阻止するために、統制を設計して実装していますか？	
サプライチェーン管理、透明性、および説明責任 障害のレポート	STA-02.1	電子的な方法 (ポータルなど) を通じて、関係するお客様やプロバイダーに対してセキュリティ事故情報を定期的に提供していますか？	AWS の事故対応プログラム、計画、および手続きは、ISO 27001 基準に合わせて作成されています。AWS レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。 詳細については、AWS クラウドセキュリティホワイトペーパー (http://aws.amazon.com/security で入手可能) を参照してください。
サプライチェーン管理、透明性、および説明責任 ネットワークおよびインフラストラクチャサービス	STA-03.1	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。
	STA-03.2	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？	
サプライチェーン管理、透明性、および説明責任 プロバイダー内部評価	STA-04.1	お客様のポリシー、手順、およびサポート対象の対策とメトリックスの準拠と効果性について内部評価を毎年行っていますか？	AWS の調達およびサプライチェーンチームは、すべての AWS サプライヤとの関係を維持しています。 詳細については、ISO 27001 基準の付録 A、ドメイン 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。
サプライチェーン管理、透明性、および説明責任 サードパーティー契約	STA-05.1	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、外注先プロバイダーを選択および監視していますか？	AWS システムとデバイスをサポートするサードパーティープロバイダーに対する従業員セキュリティ要件は、AWS の親組織である Amazon.com および各サードパーティープロバイダーとの相互機密保持契約で確立されます。Amazon リーガルカウンセルおよび AWS 調達チームが、サードパーティープロバイダーとの契約で AWS サードパーティープロバイダーの従業員セキュリティ要件を定義します。AWS の情報を扱うすべての従業員は、最低でも雇用前審査に合格し、AWS の情報へのアクセス権を付与される前に、機密保持契約書 (NDA) に署名する必要があります。 通常、AWS は請負業者に対する AWS サービスの外注開発は行っていません。
	STA-05.2	データの送信元である国の法律に従って、外注先プロバイダーを選択および監視していますか？	
	STA-05.3	リーガルカウンセルがすべてのサードパーティー契約を確認していますか？	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	STA-05.4	サードパーティー契約には、情報や資産のセキュリティと保護に関するプロビジョンが含まれていますか?	
	STA-05.5	すべてのサブプロセス契約のリストとコピーをクライアントに提供し、それを更新していますか?	
サプライチェーン管理、透明性、および説明責任 サプライチェーンガバナンスのレビュー	STA-06.1	パートナーのリスク管理およびガバナンスプロセスをレビューして、そのパートナーのサプライチェーンの他のメンバーから継承したリスクに対応していますか?	AWS では、主要なサードパーティーサプライヤーと正式な契約を締結し、ビジネスでの関係に合わせた適切なリレーションシップ管理メカニズムを実装しています。AWS のサードパーティー管理プロセスは、SOC および ISO 27001 への AWS の継続的な準拠の一環として、独立監査人によって確認されます。
サプライチェーン管理、透明性、および説明責任 サプライチェーンメトリックス	STA-07.1	プロバイダーおよびお客様（テナント）との間で該当する完全かつ正確な契約（SLA など）を維持するために、ポリシーと手順を確立し、サポート対象のビジネスプロセスおよび技術的な対策を実装していますか?	
	STA-07.2	サプライチェーン全体（アップストリーム/ダウンストリーム）でプロビジョンおよび/または条件の不履行を測定して対処する能力がありますか?	
	STA-07.3	多様なサプライヤー関係に起因するサービスレベルの矛盾や不一致を管理できますか?	
	STA-07.4	少なくとも年に 1 度、すべての契約、ポリシー、およびプロセスを確認していますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
サプライチェーン 管理、透明性、お よび説明責任 サードパーティー 評価	STA-08.1	毎年のレビューを実施することにより、情報サプライチェーン全体で妥当な情報セキュリティを確保していますか？	
	STA-8.2	毎年のレビューには、お客様の情報サプライチェーンが依存しているすべてのパートナーおよびサードパーティープロバイダーが含まれていますか？	
サプライチェーン 管理、透明性、お よび説明責任 サードパーティー の監査	STA-09.1	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 セキュリティは、外部の脆弱性脅威評価を実行するために、独立したセキュリティ会社と定期的に契約しています。AWS SOC 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。
	STA-09.2	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ーサービスはありますか？	
脅威と脆弱性の 管理 ウイルス対策およ び悪意のあるソフ トウェア対策	TVM-01.1	クラウドサービス提供をサポートするまたはそれに接続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 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 12 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。
	TVM-01.2	署名、リスト、または動作パターンを使用するセキュリティ上の脅威検出システムは、業界で受け入れられている期間内にすべてのインフラストラクチャコンポーネントで更新されていますか？	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
脅威と脆弱性の管理 脆弱性およびパッチ管理	TVM-02.1	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行っていますか?	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 クラウドセキュリティホワイトペーパーを参照してください (http://aws.amazon.com/security で入手可能)。詳細については、ISO 27001 基準の付録 A、ドメイン 12 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。
	TVM-02.2	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行っていますか?	
	TVM-02.3	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行っていますか?	
	TVM-02.4	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?	
	TVM-02.5	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?	
	TVM-02.6	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?	
脅威と脆弱性の管理 モバイルコード	TVM-03.1	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。
	TVM-03.2	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: オーストラリア信号局 (ASD) のクラウドコンピューティングに関するセキュリティ上の考慮事項への AWS の準拠

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

http://www.asd.gov.au/publications/csocprotect/Cloud_Computing_Security_Considerations.pdf を参照してください。

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

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

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

主要な領域	質問	AWS の回答
	h. SLA に含まれるスケジュールされた機能停止。SLA で保証される可用性の割合には、スケジュールされた機能停止も含まれますか？	AWS は、お客様が複数のアベイラビリティゾーンとリージョンを活用する環境を構築できるようにしており、スケジュールされた機能停止が発生する環境は運用していません。
	i. SLA の補償。SLA には、スケジュールされていないダウンタイムやデータ損失など、SLA の違反によって発生した実際の損害に関する適切な条項がありますか？	AWS は、AWS のサービスレベルアグリーメント (SLA) に従い、機能停止によって発生する可能性がある損失について、お客様に賠償を提供しています。
	j. データの完全性および可用性。ベンダーは、どのようにして冗長性やオフサイトバックアップといったメカニズムを実装してデータの破損や損失を防ぎ、データの整合性と可用性の両方を保証するのですか？	<p>AWS のデータ整合性統制は AWS SOC 1 Type II レポートに記載されているように、送信、保存、および処理を含むすべての段階でデータの整合性が維持される妥当な保証を提供しています。</p> <p>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。</p> <p>データセンターは、世界各地にクラスター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ゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。顧客は AWS の使用量を計画しながら、複数のリージョンやアベイラビリティゾーンを利用する必要があります。</p> <p>リージョンを指定する (Amazon S3 の場合) か、リージョン内のアベイラビリティゾーンを指定する (EBS の場合) ことで、データを保管する場所を選択します。Amazon Elastic Block Store (Amazon EBS) に保存されるデータは、これらのサービスの通常オペレーションの一部として、複数の物理的ロケーションで冗長的に保存されます。追加費用はかかりません。ただし、Amazon EBS レプリケーションは複数のゾーンにまたがるのではなく同じアベイラビリティゾーンに保存されます。</p> <p>Amazon S3 は極めて堅牢性の高いストレージインフラストラクチャを提供しています。オブジェクトは冗長化のため、同一の Amazon S3 リージョン内の複数施設に分散した複数のデバイスに保存されます。一旦格納されると、Amazon S3 は冗長性が失われた場合にすばやく検出して修復することによってオブジェクトの堅牢性を維持します。Amazon S3 は、チェックサムを用いて、格納されているデータの完全性を定期的に検証しています。破損が検出されると、冗長データを使用して修復されます。S3 に保存されるデータは、1 年間にオブジェクトの 99.99999999% の堅牢性と 99.9% の可用性を提供するよう設計されています。</p> <p>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 で入手可能) を参照してください。</p>

主要な領域	質問	AWS の回答
	k. データの復元。ファイル、Eメール、またはその他のデータを誤って削除した場合、バックアップからデータが部分的または完全に復元されるまでにどのくらいの時間がかかり、許容される最大時間は SLA に記載されていますか？	AWS のお客様は、お客様のデータの統制と所有権を保持します。AWS は、各リージョン内の複数のアベイラビリティゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。
	l. スケーラビリティ。ベンダーのサービスの使用を短期の通知でスケールできるようにするためにベンダーが提供する予備のコンピューティングリソースの量は、どれくらいですか？	AWS クラウドは分散され、セキュリティと復元力が高いため、潜在的に大きな拡張性があります。お客様は、使用内容に対する料金のみを支払って、拡張または縮小できます。
	m. ベンダーの変更。データを機関または別のベンダーに移動する場合や、ベンダーが突然破産したりクラウドビジネスを終了した場合に、ベンダーのロックインを回避するためにベンダーに依存しない形式でデータにアクセスするにはどうすればよいですか？ベンダーはどれくらい協力的ですか？ベンダーのストレージメディアからデータが完全に削除されることをどのようにして確認できますか？ Platform as a Service では、アプリケーションを別のベンダーまたは機関に簡単に移動するポータビリティと相互運用性を提供するために、ベンダーはどのような標準を使用していますか？	<p>お客様は、お客様のデータの統制と所有権を保持します。お客様は、AMI をエクスポートして、施設内または別のプロバイダーで使用できます (ただし、ソフトウェアのライセンス制限に従います)。詳細については、AWS セキュリティプロセスの概要ホワイトペーパー (http://aws.amazon.com/security で入手可能) を参照してください。</p> <p>AWS では、必要に応じてお客様がデータを AWS ストレージから出し入れすることを許可しています。S3 用 AWS Import/Export サービスでは、転送用のポータブル記憶装置を使用して、AWS 内外への大容量データの転送を高速化できます。AWS では、お客様がご自分のテープバックアップサービスプロバイダを使用してテープへのバックアップを実行することを許可しています。ただし、AWS ではテープへのバックアップサービスを提供していません。</p>
第三者による不正アクセスからのデータの保護	a. クラウドデプロイモデルの選択。セキュリティがより低い可能性があるパブリッククラウド、セキュリティがより高い可能性があるハイブリッドクラウド、または最もセキュリティが高い可能性があるプライベートクラウドのどれを検討したらよいですか？	<p>AWS のコンプライアンスセキュリティチームは、Control Objectives for Information and related Technology (COBIT) フレームワークに基づき、情報セキュリティフレームワークを設定しました。AWS セキュリティフレームワークは、ISO 27002 ベストプラクティスおよび PCI データセキュリティ基準を統合しています。</p> <p>詳細については、AWS リスクとコンプライアンスホワイトペーパー (http://aws.amazon.com/security で入手可能) を参照してください。AWS は、サードパーティーによる証明、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。</p>

主要な領域	質問	AWS の回答
		<p>Amazon Virtual Private Cloud (Amazon VPC) で、アマゾンウェブサービス (AWS) クラウドの論理的に分離したセクションをプロビジョニングし、ここで、お客様が定義する仮想ネットワークで AWS リソースを起動することができます。独自の IP アドレス範囲の選択、サブネットの作成、ルートテーブル、ネットワークゲートウェイの設定など、仮想ネットワーク環境を完全にコントロールできます。Amazon VPC のネットワーク設定は容易にカスタマイズすることができます。たとえば、インターネットとのアクセスが可能なウェブサーバーのパブリック サブネットを作成し、データベースやアプリケーションサーバーなどのバックエンドシステムをインターネットとのアクセスを許可していないプライベート サブネットに配置できます。セキュリティグループやネットワークアクセスコントロールリストなどの複数のセキュリティレイヤーを活用し、各サブネットの Amazon EC2 インスタンスへのアクセスをコントロールすることができます。</p> <p>加えて、既存のデータセンターと自分の VPC 間にハードウェア Virtual Private Network (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。</p>
	<p>b. データの機密性。クラウドに保存またはクラウドで処理するデータは、分類され、機密であるかプライベートである、または当社のパブリックウェブサイトからの情報など、公開されたデータですか? データの集約により、個別の各データよりも機密性が高まりますか? たとえば、大量のデータを保存したり、危害が加えられた場合にアイデンティティの盗難が容易になるさまざまなデータを保存すると、機密性が高まる可能性があります。侵害があった場合に、それへの配慮について上層部や政府役人、一般に示すことはできますか?</p>	<p>AWS のお客様は、お客様のデータの統制と所有権を有しています。また、お客様の要件に合う構造化データ分類プログラムを導入することができます。</p>

主要な領域	質問	AWS の回答
	<p>c. 法律上の義務。さまざまな法律に準拠してデータを保護、管理するための義務にはどのようなものがありますか? たとえば、プライバシー法、公文書館法、データの種類の固有のその他の法律などです。契約上、ベンダーはこれらの義務を負うことに同意し、オーストラリア政府が満足いくように義務を果たす手助けをしてくれますか?</p>	<p>AWS のお客様は、適用可能な法律および規制に準拠する範囲で AWS を使用する責任を有しています。AWS は、業界の認定およびサードパーティーによる証明、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。</p> <p>AWS はプライバシーに関するオーストラリアの考慮事項に関連して AWS の使用についてのホワイトペーパーを発行しており、こちらから入手できます。</p>
	<p>d. データにアクセスできる国。データが保存、バックアップ、処理されるのは、どの国ですか? データが経由するのはどの国ですか? フェイルオーバーや冗長性を持つデータセンターがあるのはどの国ですか? これらの質問への答えが変更された場合、ベンダーは通知してくれますか?</p>	<p>AWS のお客様は、コンテンツとサーバーを配置する 1 つ以上の AWS リージョンを選択できます。これにより、具体的な地理的要件を持っているお客様が、選択する場所で環境を構築することができます。オーストラリアの AWS のお客様は、アジアパシフィック (シドニー) リージョンに専用で AWS サービスをデプロイし、コンテンツをオーストラリア大陸内に保存することができます。お客様がこの選択を行った場合、お客様がデータの移動を選択しない限り、コンテンツはオーストラリア内に配置されます。お客様は複数のリージョンにコンテンツをレプリケートしてバックアップできますが、AWS はお客様が選択した 1 つ以上のリージョンの外部にコンテンツを移動またはレプリケートすることはありません。</p> <p>AWS はお客様のセキュリティに関して油断のない注意を払っており、召喚状や裁判所の命令、または該当する法律によって要求されるなど、法的に有効で拘束力のある命令に従う必要がある場合を除き、オーストラリア、米国、またはその他の政府からの要求に応じてデータを公開または移動することはありません。通常、米国以外の政府または規制団体は、有効で拘束力のある命令を取得するには、米国政府との相互法的援助契約など、認められた国際手順を使用する必要があります。さらに、AWS では法律で禁止される場合を除き、可能な場合はコンテンツを公開する前にお客様に通知し、お客様が公開からの保護手段を探せるようにしています。</p>

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

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

主要な領域	質問	AWS の回答
	<p>j. ゲートウェイテクノロジー。安全なゲートウェイ環境を作成するために、ベンダーはどのようなテクノロジーを使用していますか？この例には、ファイアウォール、トラフィックフローフィルター、コンテンツフィルター、および該当する場合はウイルス対策ソフトウェアやデータダイオードがあります。</p>	<p>AWS ネットワークは、既存のネットワークセキュリティの問題に対する強固な保護機能を備えており、お客様はさらに堅牢な保護を実装することができます。詳細については、AWS 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。</p> <p>Amazon の資産 (ノートパソコンなど) は、E メールフィルタリングとマルウェア検出を含むウイルス対策ソフトウェアで設定されています。</p> <p>AWS ネットワークファイアウォール管理および Amazon のウイルス対策プログラムは、SOC、PCI DSS、ISO 27001、および FedRAMPsm への AWS の継続的な準拠の一環として、第三者の独立監査人によって確認されます。</p>
	<p>k. ゲートウェイの認定。ベンダーのゲートウェイ環境は政府のセキュリティ標準や規制に対して認定されていますか？</p>	<p>AWS は、AWS ゲートウェイ環境を含む、業界の認定と独立したサードパーティーによる証明を取得します。</p>
	<p>l. E メールコンテンツのフィルタリング。Eメールの Software as a Service では、ベンダーは機関の Eメールコンテンツポリシーを適用できる、カスタマイズ可能な Eメールコンテンツフィルタリングを提供していますか？</p>	<p>お客様はシステムを利用して Eメール機能をホストできますが、その場合、Eメールの出入力ポイントで適切なレベルのスパムおよびマルウェア保護を採用し、新しいリリースが利用可能になったらスパムとマルウェアの定義を更新するのはお客様の責任です。</p>
	<p>m. ベンダーの IT セキュリティ体制をサポートするポリシーとプロセス。ベンダーのコンピュータおよびネットワークセキュリティ体制が、脅威とリスク評価、継続的な脆弱性管理、セキュリティを組み込んだ変更管理プロセス、侵入テスト、ログおよび定期的なログ分析、オーストラリア政府が支持するセキュリティ製品の使用、オーストラリア政府のセキュリティ標準や規制への準拠を含むポリシーやプロセスによってどのようにサポートされているかの詳細情報を入手できますか？</p>	<p>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。</p> <p>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 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。</p> <p>AWS のお客様は、AWS が管理する主な統制を指定できます。主な統制はお客様の統制環境にとって不可欠であり、年次の会計監査などのコンプライアンス要件に準拠するには、その主な統制の運用効率について外部組織による証明が必要です。そのために、AWS は Service Organization Controls 1 (SOC 1) Type II レポートで幅広く詳細な IT 統制を公開しています。SOC 1 レポートの旧称は Statement on Auditing Standards (SAS) No. 70、Service Organizations レポートです。以前は Statement on Standards for Attestation Engagements No. 16 (SSAE 16) レポートと呼ばれ、米国公認会計士協会 (AICPA) が作成し、幅広く認められている監査基準です。SOC 1 監査は、AWS で定義している統制目標および統制活動 (AWS が管理するインフラストラクチャの一部に対する統制目標と統制活動が含まれます) の設計と運用効率の両方に関する詳細な監査です。「Type II」は、レポートに記載されている各統制が、統制の妥当性に関して評価されるだけでなく、運用効率についても外部監査人によるテスト対象であることを示します。AWS の外部監査人は独立し、適格であるため、レポートに記載されている統制は、AWS の統制環境に高い信頼を置けることを示します。</p>

主要な領域	質問	AWS の回答
	<p>n. ベンダーの IT セキュリティ体制をサポートするテクノロジー。ベンダーのコンピュータおよびネットワークセキュリティ体制が、セキュリティパッチのタイムリーな適用、ウイルス対策ソフトウェアの定期的な更新、不明な脆弱性に対する保護のための深層防御メカニズム、可能な限り強力なセキュリティ設定で強化されたオペレーティングシステムとソフトウェアアプリケーション、侵入検出/防止システム、およびデータ損失防止メカニズムを含む直接的な技術統制によってどのようにサポートされているかに関する詳細情報を入手できますか?</p>	<p>AWS は、サードパーティーによる証明、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。</p> <p>AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします (お客様のインスタンスはこのスキャンの対象外です)。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、脆弱性に対する外部からの脅威の査定が、独立系のセキュリティ会社によって定期的に行われます。これらの査定に起因する発見や推奨事項は、分類整理されて AWS 上層部に報告されます。</p> <p>さらに、AWS 統制環境は、通常の内部的および外部的リスク評価によって規定されています。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。</p>
	<p>o. ベンダーの IT セキュリティ体制の監査。当社に提供された環境のスキャンおよびその他の侵入テストの実行を含む、ベンダーのセキュリティ手法の実装を監査できますか? 監査が可能でないという正当な理由がある場合、どの信頼できるサードパーティーが監査やその他の脆弱性評価を実行しましたか? ベンダーが実施する内部監査の種類と、それらの評価に使用されるコンプライアンス標準と組織の推奨の手法 (クラウドセキュリティアライアンスなど) は何ですか? 最近の結果レポートのコピーを詳細に確認することはできますか?</p>	<p>AWS は、サードパーティーによる証明、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。</p> <p>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。</p> <p>AWS Security は、外部の脆弱性脅威評価を実行するために、独立したセキュリティ会社と定期的に契約しています。AWS SOC 1 Type 2 レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。</p>

主要な領域	質問	AWS の回答
	<p>p. ユーザーの認証。Software as a Service を使用するためのユーザーのログインのためにベンダーがサポートするアイデンティティ & アクセス管理システムは何ですか?</p>	<p>AWS Identity and Access Management (IAM) により、お客様のユーザーの AWS サービスおよびリソースへのアクセスを安全にコントロールすることができます。IAM を使用すると、AWS のユーザーとグループを作成および管理し、アクセス権を使用して AWS リソースへのアクセスを許可および拒否できます。</p> <p>AWS は、ユーザーの ID を 1 つの場所に維持することで、ユーザーの管理を容易にする ID フェデレーションをサポートしています。AWS IAM には SAML (Security Assertion Markup Language) 2.0 のサポートが含まれます。これは、多くの ID プロバイダーにより使用されているオープンスタンダードです。この新機能によりフェデレーティッドシングルサインオン (SSO) が可能になり、Shibboleth や Windows Active Directory フェデレーションサービスなどの SAML 準拠の ID プロバイダーと連携して、ユーザーが AWS マネジメントコンソールにログインしたり、AWS API をプログラムで呼び出したりすることができるようになります。</p>
	<p>q. データのコントロールの中央集約化。機関のユーザーが、信頼された運用環境以外で未承認または安全でないコンピューティングデバイスを使用して、Software as a Service で機密のデータを保存または処理できないようにするユーザートレーニング、ポリシー、技術統制は何ですか?</p>	<p>該当なし</p>
	<p>r. ベンダーの物理的なセキュリティ体制。ベンダーは、オーストラリア政府によって支持される物理的なセキュリティ製品やデバイスを使用していますか? ベンダーの物理データセンターはどのようにしてサーバー、インフラストラクチャ、およびそれらに保存されたデータの改ざんや盗難を防止するように設計されていますか? ベンダーの物理的なデータセンターは権威あるサードパーティーによって認定されていますか?</p>	<p>AWS 定義の論理統制と物理統制の定義は、SOC 1 Type II レポートに文書化されています。また、このレポートは、この監査チームとコンプライアンスチームのレビューに使用できます。また、AWS ISO 27001 およびその他の認定も、監査人のレビュー用に使用できます。</p> <p>物理的セキュリティ統制には、フェンス、壁、保安要員、監視カメラ、侵入検知システムその他の電子的手段による周辺統制が含まれますが、これに限定されるものではありません。物理的アクセスは、建物の周辺および入り口において、監視カメラや侵入検知システムなどの電子的手段を用いる専門の保安要員その他の手段により、厳重に管理されています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。サーバー設置箇所への物理アクセスポイントは、AWS データセンター物理セキュリティポリシーの規定により、閉回路テレビ (CCTV) カメラで録画されています。録画は 90 日間保存されます。ただし、法的または契約義務により 30 日間に制限される場合もあります。</p> <p>AWS は、このような特権を必要とする正規の業務を有する承認済みの従業員や契約社員に対して、データセンターへの物理的なアクセス権や情報を提供しています。すべての訪問者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが付き添いを行います。</p> <p>物理的なアクセス、データセンターへのアクセスの承認、その他の関連統制については、SOC 1 Type II レポートを参照してください。</p>

主要な領域	質問	AWS の回答
	<p>s. ソフトウェアとハードウェアの調達。クラウドインフラストラクチャソフトウェアとハードウェアが正当なソースから供給され、配送中に悪意を持って変更されないようにするために、どのような調達プロセスが使用されていますか?</p>	<p>詳細については、ISO 27001 基準の付録 A、ドメイン 9.1 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。</p> <p>ISO 27001 基準に合わせて、AWS の担当者が AWS 専有インベントリ管理ツールを使用して、AWS ハードウェアの資産に所有者を割り当て、追跡および監視を行っています。AWS の調達およびサプライチェーンチームは、すべての AWS サプライヤとの関係を維持しています。</p> <p>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。</p>
ベンダーの顧客による不正アクセスからのデータの保護	<p>a. 顧客の区別。複数のテナント間で仮想化と "マルチテナンシー" メカニズムが適切な論理的分離とネットワークの分離を保証し、当社と同じ物理的なコンピュータを使用中の悪意を持った顧客がデータにアクセスできないようにするために、どのような保証がありますか?</p> <p>b. セキュリティ体制の低下。ベンダーによるクラウドインフラストラクチャの使用は、機関の既存のネットワークセキュリティ体制を低下させますか? ベンダーは当社の明示的な同意なしに顧客の 1 社として当社を宣伝し、それが当社を対象とした攻撃につながることはありますか?</p> <p>c. 専用サーバー。当社の仮想マシンを実行する物理的なコンピュータに対してなんらかの制御を得ることはできますか? 追加の料金を支払って、当社と同じ物理的なコンピュータ (専用サーバーや仮想プライベートクラウドなど) を他の顧客が使用しないようにすることはできますか?</p>	<p>現在、Amazon EC2 は、高度にカスタマイズされたバージョンの Xen ハイパーバイザーを利用しています。ハイパーバイザーは、社内および社外の侵害対策チームによって新規および既存の脆弱性と攻撃進路を定期的に評価しています。また、ゲスト仮想マシン間の強力な隔離を維持するためにも適しています。AWS Xen ハイパーバイザーのセキュリティは、評価および監査の際に独立監査人によって定期的に評価されています。</p> <p>AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。お客様が自身のデータの統制と所有権を有しているため、データの暗号化を選択するのはお客様の責任です。AWS では、S3、EBS、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC セッションも暗号化されます。また、Amazon S3 は、お客様向けのオプションとしてサーバー側の暗号化も提供しています。詳細については、AWS リスクとコンプライアンスホワイトペーパー (http://aws.amazon.com/security) を参照してください。</p> <p>AWS のお客様は機密であると見なされ、AWS が明示的な同意なくお客様の詳細を公表することはありません。Amazon Virtual Private Cloud (Amazon VPC) で、アマゾンウェブサービス (AWS) クラウドの論理的に分離したセクションを確保し、ここで、お客様が定義する仮想ネットワークで AWS リソースを起動することができます。独自の IP アドレスレンジの選択、サブネットの作成、ルートテーブル、ネットワークゲートウェイの設定など、仮想ネットワーク環境を完全にコントロールできます。</p> <p>VPC により、お客様はハードウェアレベルで物理的に切り離されている Amazon EC2 インスタンスを起動でき、インスタンスはシングルテナントのハードウェアで実行されます。VPC は、「専用」テナンシーで作成できます。この場合、その VPC に対して起動されたインスタンスすべてがこの機能を利用します。また、「デフォルト」テナンシーで作成することもできますが、VPC に対して起動された特定のインスタンスについては、顧客が「専用」テナンシーを指定します。</p>

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

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

主要な領域	質問	AWS の回答
	c. ベンダーの従業員のトレーニング。ベンダーのシステムの安全な使用方法について知り、セキュリティインシデントの可能性を認識するために、ベンダーの従業員が必要とする資格、認定、定期的な情報セキュリティの認識は何ですか？	ISO 27001 基準に合わせて、すべての AWS 従業員は、修了時に承認を必須とする定期的な情報セキュリティトレーニングを修了しています。従業員が制定されたポリシーを理解し遵守していることを確認するために、コンプライアンス監査を定期的実施しています。詳細については、AWS セキュリティプロセスの概要ホワイトペーパー (http://aws.amazon.com/security) を参照してください。
	d. セキュリティインシデントの通知。同意されたしきい値よりも深刻なセキュリティインシデントについて、ベンダーは安全な通信で通知してくれますか (特に、ベンダーに責任がある可能性が高い場合)? ベンダーは、当社のデータの保存または処理に使用するコンピューティング機器を差し押さえる可能性がある法律執行機関または他の機関に自動的に通知を行いますか？	セキュリティインシデントの通知はケースバイケース、および該当する法律で要求される場合に処理されます。すべての通知は安全な通信で行われます。
	e. ベンダーサポートの範囲。データの不正な公開などのセキュリティ違反、または法的な電子開示や証拠提示を行う必要がある場合に、ベンダーはどの程度調査に協力してくれますか？	AWS はインフラストラクチャを提供し、その他の部分はお客様が管理します。たとえば、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典、収集、処理、分析、および作成に関連する法的手続きに、適切に対応する責任を持ちます。法的手続きに AWS の協力を必要とするお客様には、AWS は要請に応じて連携をとります。
	f. ログへのアクセス。フォレンジック調査を実行するために、時間を同期した監査ログやその他のログにアクセスする方法と、裁判所での適切な証拠となるようにログが作成および保存される方法は何ですか？	<p>お客様は、自身のゲストオペレーティングシステム、ソフトウェア、アプリケーションの統制を有しており、これらのシステムの状態の論理的なモニタリングを開発するのは、お客様の責任です。AWS 情報システムは、ISO 27001 基準に合わせて、NTP (Network Time Protocol) を介して同期される内部システムクロックを利用しています。</p> <p>AWS CloudTrail は、複雑なログシステムを実行する負荷の軽減に役立つ、ログユーザーアクティビティのシンプルなソリューションを提供します。詳細については、aws.amazon.com/cloudtrail を参照してください。</p> <p>AWS CloudWatch は、AWS 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のモニタリングを提供します。詳細については、aws.amazon.com/cloudwatch を参照してください。また、AWS は、サービス状態ダッシュボード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。</p>
	g. セキュリティインシデントの補償。ベンダーのアクション、問題のあるソフトウェア、またはハ-	AWS の事故対応プログラム、計画、および手続きは、ISO 27001 基準に合わせて作成されています。AWS SOC 1 Type 2 レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。

主要な領域	質問	AWS の回答
	ドウェアがセキュリティ違反の原因となった場合、ベンダーはどのようにして適正な補償を行いますか？	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 で入手可能) を参照してください。
	h. データスピル。クラウドに保存するには機密性が高すぎると当社が考えるデータが誤ってクラウドに保存され、データスピルとして参照された場合、フォレンジックなサニタイズ手法を使用して、書き出されたデータをどのように削除できますか？ データを削除するたびに、物理ストレージメディアの該当する部分はゼロで埋められますか？ そうでない場合、削除されたデータが通常の操作の一部として顧客によって上書きされるのにどのくらい長かかりますか？ 通常、クラウドには未使用のストレージ容量が多く用意されています。漏えいしたデータをベンダーのバックアップメディアからフォレンジックに削除できますか？ 書き出されたデータは他にどこに保存されますか？ また、それをフォレンジックに削除することはできますか？	<p>お客様は、お客様のコンテンツの所有権と統制を有しています。AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。AWS では、S3、EBS、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC への IPsec トンネルも暗号化されます。また、Amazon S3 は、お客様向けのオプションとしてサーバー側の暗号化も提供しています。詳細については、AWS リスクとコンプライアンスホワイトペーパー (http://aws.amazon.com/security) を参照してください。</p> <p>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。</p>

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

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

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

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

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

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

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働させることができるようにするものです。

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

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

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

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

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

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

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

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

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

SAS 70: Statement on Auditing Standards No. 70:Service Organizations は、Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) が発行する監査書です。SAS 70 は、サービス監査人がサービス組織 (AWS など) の内部統制を評価し、サービス監査人のレポートを発行する際の指針を示しています。また、SAS 70 は、1 つまたは複数のサービス組織を使用する組織の財務諸表の監査人に対する指針も示しています。SAS 70 レポートは、Service Organization Controls 1 レポートに変更されました。

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

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

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

SSAE 16 [廃止]: 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、ウェブサイトにてシールとして掲載したりすることができます。

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

バージョン履歴

2015 年 12 月

- 「認定とサードパーティーによる証明」のサマリを更新しました
- ISO 27017 認定を追加しました
- ISO 27018 認定を追加しました
- 11 番目のリージョンを追加しました (中国北京)

2015 年 11 月

- CSA v3.0.1 に更新しました

2015 年 8 月

- PCI 3.1 の対象サービスを更新しました
- PCI 3.1 の対象リージョンを更新しました

2015 年 5 月

- 10 番目のリージョンを追加しました (欧州フランクフルト)
- SOC 3 の対象サービスを更新しました
- SSAE 16 の言語を廃止しました

2015 年 4 月

- FedRAMPsm、HIPAA、SOC 1、ISO 27001、ISO 9001 の対象サービスを更新しました

2015 年 2 月

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

2014 年 12 月

- 「認定とサードパーティーによる証明」のサマリを更新しました

2013 年 11 月バージョン

- IPsec トンネル暗号化用語を編集しました

2013 年 6 月バージョン

- 「認定とサードパーティーによる証明」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ーによる証明」のサマリを編集しました

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ーによる証明」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

注意

© 2010-2016 Amazon.com, Inc., or its affiliates. 本文書は、情報提供の目的のみにために提供されるものです。本文書は、本文書の発行日時点での、AWS の提供商品を紹介するものであり、これらは事前の通知なく変更される場合があります。お客様は本文書の情報および AWS 製品の使用について独自に評価する責任を負うものとし、これらの情報は、明示または黙示を問わずいかなる保証も伴うことなく、「現状のまま」提供されるものです。本文書内のいかなるものも、AWS、その関係者、サプライヤ、またはライセンサーからの保証、表明、契約的なコミットメント、条件や確約を意味するものではありません。お客様に対する AWS の責任は AWS 契約によって規定されています。また、本文書は、AWS とお客様との間の契約に属するものではなく、また、当該契約が本文書によって修正されることもありません。