CSA Consensus Assessments Initiative Questionnaire

2017 年 1 月

注意

本文書は情報提供のみを目的としています。本文書は、発行時点における AWS の製品と対応を説明するものであり、予告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 製品またはサービスの利用について、ご自身の評価に基づき判断する責任を負います。いずれの AWS 製品またはサービスも、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」提供されます。本文書のいかなる内容も、AWS とその関係会社、サプライヤー、またはライセンサーからの保証、表明、および契約上の責任、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 とお客様との間のいかなる契約の一部も構成するものではなく、また、当該契約が本文書によって変更されることもありません。

目次

要約

CSA Consensus Assessments Initiative Questionnaire には、クラウド利用者およびクラウド監査人からクラウドプロバイダーへの質問として CSA が想定しているものが挙げられています。質問は、セキュリティ、統制、およびプロセスに関する一連の事項を含み、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。これらの質問に対する AWS の回答については、本文書の次章以降を参照ください。

はじめに

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確保に向けたベストプラクティスの使用を促進するとともに、クラウドコンピューティングの利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ことを目標とする非営利組織」です。詳細については、https://cloudsecurityalliance.org/about/ を参照してください。

この目標を達成するために、多岐にわたる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

統制グループ	CID	コンセンサス評価の質問	AWS の回答
アプリケーションとインターフェイスのセキュリティ アプリケーションのセキュリティ	AIS-01.1	業界標準 (Build Security in Maturity Model [BSIMM] Benchmarks、Open Group ACS Trusted Technology Provider Framework、NIST など) を利用して、システム/ソフトウェア開発ライフサイクル (Systems/Software Development Lifecycle/SDLC) にセキュリティを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確立しています。詳細については、ISO 27001 規格の附属書 A ドメイン

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	AIS-01.2	運用前にコードのセキュリティ上の不具合を検出するために、自動ソースコード分析ツールを利用していますか?	14 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
	AIS-01.3	運用前にコードのセキュリティ上の不具合を検出するために、手動ソースコード分析を利用していますか?	
	AIS-01.4	すべてのソフトウェアサプライヤーが、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標準に従っていることを確認していますか?	
	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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
アプリケーションとインターフェイスのセキュリティ 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指定されたセキュリティ、契約、および規制の要件は、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、適用される法律および規制に準拠する範囲で AWS を使用する責任を有しています。AWS は、業界の認証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、認証、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	顧客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?	
アプリケーションとインターフェイスのセキュリティ 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ースおよびデータベースについてデータの入力と出力の整合性ルーチン (一致チェック、編集チェックなど) が実装されていますか?	AWS のデータ整合性統制は AWS SOC 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 規格の附属書 A ドメイン 14 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
アプリケーションとインターフェイスのセキュリティ 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、業界標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、業界のベストプラクティスを組み込むように設計されています。 AWS が実施している各種ベストプラクティスの詳細については、AWS 認証、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)。
監査、保証、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フォーマット (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、複数の業界認証と独立したサードパーティーによる保証を取得しており、特定の認証や関連する文書を AWS のお客様に直接提供しています。
監査保証、コンプライアンス 独立した監査	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証レポートを閲覧す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保証、認証、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 のもとお客様に直接提供しています。 AWS ISO 27001 認証はこちらからダウンロードできます。 AWS SOC 3 レポートはこちらからダウンロードできます。 AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャ
	AAC-02.2	業界のベストプラクティスおよびガイダンスに従い、クラウドサービスインフラストラクチャのネットワーク侵入テストを定期的に実行していますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	AAC-02.3	業界のベストプラクティスおよびガイダンスに従い、クラウドインフラストラクチャのアプリケーション侵入テストを定期的に実行していますか?	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、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。 さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。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ガイダンスに従い、内部監査を定期的に実行していますか?	
	AAC-02.5	業界のベストプラクティスおよびガイダンスに従い、外部監査を定期的に実行していますか?	
	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?	
	AAC-02.7	内部監査および外部監査の結果は、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	部門横断的な評価の監査が可能な内部監査プログラムを実施していますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
監査、保証、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ので、データの暗号化を選択するのはお客様の責任です。AWS では、S3、EBS、SimpleDB、EC2 など、ほぼすべてのサービスについて、お客様

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	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?	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、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。 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。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	AAC-03.3	顧客データの保存を特定の国や地理的な場所に制限することができますか?	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ません。使用できるリージョンの完全なリストについては、AWS グローバルインフラストラクチャのページを参照してください。
	AAC-03.4	該当する司法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 規格の附属書 A ドメイン 18 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
事業継続管理と運用レジリエンス 事業継続計画	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ーゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。顧客は AWS の使用量を計画しながら、複数のリージョンやアベイラビリティーゾーンを利用する必要があります。 詳細については、AWS 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。
	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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
事業継続管理と運用レジリエンス 事業継続テスト	BCR-02.1	事業継続計画の有効性を保持するために、スケジュールした間隔で、または組織または環境の重大な変更時に、計画をテストしていますか?	AWS の事業継続ポリシーおよび計画は、ISO 27001 規格に合わせて開発され、テストされています。 AWS と事業継続の詳細については、ISO 27001 規格の附属書 A ドメイン 17 を参照してください。
事業継続管理と運用レジリエンス 電力および電気通信	BCR-03.1	システム間のデータの移送経路を示す文書を、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。
	BCR-03.2	テナントは、データの移送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?	
事業継続管理と運用レジリエンス ドキュメント	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、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。 また、ISO 27001 附属書 A ドメイン 12 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
事業継続管理と運用レジリエンス 環境リスク	BCR-05.1	破損 (自然の原因、災害、意図的な攻撃などによる) に対する物理的な保護が予測および設計され、対策が適用されていますか?	AWS のデータセンターは、環境リスクに対する物理的な保護を組み込んでいます。環境リスクに対する AWS の物理的な保護は、独立監査人によって検証され、ISO 27002 のベストプラクティスに準拠していると認証されました。 詳細については、ISO 27001 規格の附属書 A ドメイン 11 を参照してください。
事業継続管理と運用レジリエンス 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証されました。詳細については、ISO 27001 規格の附属書 A ドメイン 11 を参照してください。
事業継続管理と運用レジリエンス 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、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。
	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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	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行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
事業継続管理と運用レジリエンス 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 規格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 認証規格への対応を確認する独立監査人から、審査および認証を受けています。 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 で入手可能) を参照してください。
事業継続管理と運用レジリエンス 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クス (CSA、CAMM など) をテナントが利用できるようにしていますか?	
	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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
事業継続管理と運用レジリエンス 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 の要件に基づいて、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。
事業継続管理と運用レジリエンス 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、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。 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 規格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 規格の附属書 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?	
変更制御と設定管理 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 の要件に基づいて、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「AWS ドキュメント」セクション (https://aws.amazon.com/documentation/) 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記述した文書はありますか?	
変更制御と設定管理 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ありますか?	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 規格の附属書 A ドメイン 14 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
	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不具合を検出する統制はありますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
変更制御と設定管理 品質テスト	CCC-03.1	品質保証プロセスについて記述した文書をテナントに提供していますか?	AWS は ISO 9001 認証を維持しています。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。 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。 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。 また、詳細については、ISO 27001 規格の附属書 A ドメイン 14 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
	CCC-03.2	特定の製品/サービスに関する既知の問題を記述した文書はありますか?	
	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?	
	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削除されていることを保証するための仕組みはありますか。	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
変更制御と設定管理 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ありますか?	悪意のあるソフトウェアに対する AWS のプログラム、プロセス、および手続きは、ISO 27001 規格に合わせています。 詳細については、ISO 27001 規格の附属書 A ドメイン 12 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
変更制御と設定管理 運用の変更	CCC-05.1	運用変更管理手続きとその役割/権限/責任について記述した文書を、テナントに提供していますか?	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。 また、詳細については、ISO 27001 規格の附属書 A ドメイン 12 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
データのセキュリティと情報ライフサイクルの管理 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、使用す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。AWS リージョンの最新の一覧については、AWS グローバルインフラストラクチャのページを参照してください。
	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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	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。AWS リージョンの最新の一覧については、AWS グローバルインフラストラクチャのページを参照してください。
データのセキュリティと情報ライフサイクルの管理 データインベントリ/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。AWS リージョンの最新の一覧については、AWS グローバルインフラストラクチャのページを参照してください。
	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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
データのセキュリティと情報ライフサイクルの管理 *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、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。
	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?	
データのセキュリティと情報ライフサイクルの管理 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保持します。また、お客様は、お客様の要件に合うラベリングおよび処理に関するポリシーおよび手続きを実装できます。
	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
データのセキュリティと情報ライフサイクルの管理 非運用データ	DSI-05.1	運用データが非本番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、お客様が本番環境および非本番環境を保守および開発できるようにしています。運用データが非本番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。
データのセキュリティと情報ライフサイクルの管理 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。
データのセキュリティと情報ライフサイクルの管理 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?	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 クラウドセキュリティホワイトペーパー

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。	(http://aws.amazon.com/security で入手可能) を参照してください。 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、特定の方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。 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 ストレージとの間を移動するデータが暗号化されます。この処理を効率的かつ低レイテンシーで行うために、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) でのみ使用できます。

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 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 規格に合わせて、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 サプライヤーとの関係を維持しています。 詳細については、ISO 27001 規格の附属書 A、ドメイン 8 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
	DCS-01.2	重要なサプライヤー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、それら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 規格の附属書 A、ドメイン 11 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
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 規格に合わせて機器識別を管理しています。 AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
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、事業継続のため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、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。
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 規格に合わせて、AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。 詳細については、ISO 27001 規格の附属書 A、ドメイン 8 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
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 規格の附属書 A、ドメイン 11 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
	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 規格に合わせて、すべての AWS 従業員は、修了時に承認を必須とする定期的な情報セキュリティトレーニングを修了しています。従業員が制定されたポリシーを理解し遵守していることを確認するために、コンプライアンス監査を定期的に実施しています。詳細については、AWS 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。 AWS は、ISO 27001 認証への対応を確認する独立監査人から、審査および認証を受けています。また、AWS SOC 1 および SOC 2 レポートにも詳細な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
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。AWS リージョンの最新の一覧については、AWS グローバルインフラストラクチャのページを参照してください。
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。 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。
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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
暗号化とキーの管理 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、ホストで必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。 AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠のために、サードパーティーの独立監査人によって確認されます。
暗号化とキーの管理 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はありますか?	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
	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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	EKM-02.3	キー管理手続きを維持していますか?	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。 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。 AWS は、AWS インフラストラクチャ内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。AWS は NIST で承認されたキー管理テクノロジーとプロセスを AWS 情報システムで使用して対称暗号キーを作成、管理、配布しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストで必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。 AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠のために、サードパーティーの独立監査人によって確認されます。
	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?	
	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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
暗号化とキーの管理 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)。KMS の詳細については、AWS SOC レポートを参照してください。 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-03.2	ネットワークおよびハイパーバイザーインスタンス間の移送時に、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?	
	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文書はありますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
暗号化とキーの管理 ストレージとアクセス	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。 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。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストで必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。 AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠のために、サードパーティーの独立監査人によって確認されます。
	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?	
	EKM-04.3	暗号化キーをクラウドに保管していますか?	
	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?	

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 規格に合わせて重要なコンポーネントのシステムの基礎を保守しています。詳細については、ISO 27001 規格の附属書 A、ドメイン 14 および 18 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。 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証を発行して、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。関連する認証とレポートを 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。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	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?	AWS は、ISO 27001 規格に合わせて、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。加えて、AWS は AWS ISO 27018 認証を維持しています。ISO 27018 に準拠することにより、AWS はお客様のコンテンツのプライバシー保護に特に対応したコントロールシステムを設けていることを示しています。詳細については、AWS Compliance ISO 27018 FAQ http://aws.amazon.com/compliance/iso-27018-faqs/ を参照してください。
ガバナンスおよびリスク管理 管理の監視	GRM-03.1	技術管理者、業務管理者、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、当社のシニアマネジメント層で開始されます。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 認証を提供しています。ISO 27001 認証は特に 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。認証とは、サードパーティーによる認定を受けた独立監

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	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?	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 認証規格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/
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 認証可能なフレームワークを実質的に統合しています。 AWS は、ISO 27001 規格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。 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。 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/ のウェブサイトに一般公開されています。
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、業界標準 (ISO-27001、ISO-22307、CoBIT など) に準拠していますか?	
	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?	
	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?	

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、認証、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、正式な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、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。 また、ISO 27001 規格の附属書 A ドメイン 7 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
	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 規格に合わせて年に 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 認証に準拠している旨の審査と認証を受けています。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
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 (http://aws.amazon.com/security で入手可能) 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/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。
ガバナンスおよびリスク管理 評価	GRM-10.1	正式なリスク評価は、エンタープライズ全体のフレームワークに適合し、少なくとも年に 1 回または計画した間隔で実行し、定性的および定量的な方法を使用して、すべての特定されたリスクの可能性と影響を判断していますか?	AWS は、ISO 27001 に合わせて、リスク管理プログラムを開発してリスクを軽減し、管理しています。 AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。 AWS のリスク管理フレームワークの詳細については、AWS リスクとコンプライアンスホワイトペーパー (http://aws.amazon.com/compliance で入手可能) を参照してください。
	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	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?	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。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
プログラム	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?	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、戦略的事業計画を持っています。また、少なくとも半年に一度、戦略的事業計画を再評価します。このプロセスでは、マネジメントがその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。 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。
人事 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?	AWS のお客様は、プライバシー違反についてお客様の環境を監視する責任を有します。 AWS SOC 1 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。
	HRS-01.2	プライバシーポリシーは、業界標準に合わせていますか?	
人事 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、経歴検証のための統制に関する追加の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
人事 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制御に関して、従業員を特別にトレーニングしていますか?	ISO 27001 規格に合わせて、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に実施しています。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、顧客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日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?	
人事 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。 詳細については AWS SOC レポートに記載されています。

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 の人事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 規格の附属書 A ドメイン 7 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
人事 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。
人事 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。
人事 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 (http://aws.amazon.com/security で入手可能) および 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。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
人事 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。 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。 詳細情報については、ISO 27001 規格および 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証を受けています。
	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?	
	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?	
人事 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式な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 規格に合わせて、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。 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。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	HRS-09.2	管理者およびデータスチュワード（データ責任者）は、セキュリティおよびデータ完全性に関する自身の法的責任について、適切な教育をうけていますか?	
人事 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 イントラネットを介した情報の電子メールメッセージおよび投稿が含まれます。詳細については、ISO 27001 規格の附属書 A ドメイン 7 および 8 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。さらに、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 で入手可能) を参照してください。
	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?	
	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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
人事 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 規格に合わせて作成しています。詳細については、ISO 27001 規格の附属書 A ドメイン 8 および 9 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。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。 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-11.2	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?	
	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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
Identity & Access Management 監査ツールのアクセス	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 規格に合わせて、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式なポリシー、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 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。

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) を監視し、ログを取得していますか?	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。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。 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。 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。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
Identity & Access Management 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くなったシステムアクセス権を適時に削除する統制はありますか?	AWS SOC レポートには、ユーザーアクセスの失効について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 規格の附属書 A ドメイン 9 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
	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の削除に要する時間を追跡するためのメトリクスを提供していますか?	
Identity & Access Management 診断および設定ポートのアクセス	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?	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。
Identity & Access Management 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 ID 情報を、アクセスレベルも含めて管理および保存していますか?	
	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 ID 情報を、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
Identity & Access Management 役割分担	IAM-05.1	クラウドサービス内で職務の分離がどのように維持されているかについて、文書をテナントに提供していますか?	お客様は、AWS リソースの役割分担を管理することができます。 AWS 社内では ISO 27001 規格に準拠した役割分担を行っています。詳細については、ISO 27001 規格の附属書 A ドメイン 6 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
Identity & Access Management 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、権限を持つ担当者にのみアクセスを制限していますか?	AWS は、ISO 27001 規格に合わせて、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式なポリシーおよび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確立した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、権限を持つ担当者にのみアクセスを制限していますか?	
Identity & Access Management	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ーゾーンだけでなく、複数の

統制グループ	CID	コンセンサス評価の質問	AWS の回答
サードパーティのアクセス	IAM-07.2	上流のプロバイダーの障害について、プロバイダーのサービス継続性を監視していますか?	地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。各アベイラビリティーゾーンは、独立した障害ゾーンとして設計されています。障害時には、自動プロセスが、顧客データの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 規格の附属書 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 認証に準拠している旨の審査と認証を受けています。
	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概要情報に顧客がアクセスできるようにしていますか?	
	IAM-07.5	テナントが災害を通知する機能を提供していますか?	
	IAM-07.6	テナントがフェイルオーバーオプションを開始する方法を提供していますか?	
	IAM-07.7	事業継続性および冗長性の計画をテナントと共有していますか?	
Identity & Access Management	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

統制グループ	CID	コンセンサス評価の質問	AWS の回答
ユーザーアクセスの制限および承認	IAM-08.2	アクセス制御のため、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提供していますか?	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。
Identity & Access Management 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、顧客 (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、ユーザーアクセスを承認し、また適切に制限していますか?	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、依頼者の 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依頼者に提供されます。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	IAM-09.2	申請があった場合、ユーザー (従業員、請負業者、顧客 (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。すべての認証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発見的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。
Identity & Access Management 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) について、権限の確認を少なくとも 1 年に 1 度実施していますか?	ISO 27001 規格に合わせて、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。 詳細については、ISO 27001 規格の附属書 A ドメイン 9 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
	IAM-10.2	ユーザーの権限が不適切であると判明した場合、すべての是正措置および確認作業は記録されますか?	
	IAM-10.3	テナントデータに対して不適切な権限が許可されていた場合、是正措置および確認作業の報告書をテナントと共有しますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
Identity & Access Management ユーザーアクセスの失効	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 の人事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 規格の附属書 A ドメイン 9 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
	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?	
Identity & Access Management 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?	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 への委任アクセスのため
	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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	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?	の 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。
	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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	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。
	IAM-12.9	テナントおよび顧客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こと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) を設けていいますか?	
Identity & Access Management 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 規格に合わせて、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。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	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?	詳細については、http://aws.amazon.com/security で入手可能な「AWS セキュリティプロセスの概要」を参照してください。
	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と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、およびインシデント対応を容易にするために、ファイルの完全性 (ホスト) およびネットワークの侵入検出 (IDS) ツールは実装されていますか?	AWS インシデント対応プログラム (事故の検出、調査、および対応) は、ISO 27001 規格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、http://aws.amazon.com/security で入手可能な「AWS セキュリティプロセスの概要」を参照してください。
	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していますか?	AWS 情報システムは、ISO 27001 規格に合わせて、NTP (Network Time Protocol)

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	IVS-01.5	セキュリティイベントについて、監査記録を (自動化ツールなどで) 定期的にレビューしていますか?	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 認証規格への対応を確認する独立監査人から、審査および認証を受けています。 AWS は、自動モニタリングシステムを活用して、ハイレベルなサービスパフォーマンスと可用性を提供します。内部的、外部的両方の使用において、様々なオンラインツールを用いたプロアクティブな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により、アラームが迅速かつ確実に運用担当者に届きます。 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。
インフラストラクチャと仮想化セキュリティ 変更検出	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、使用す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

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	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) によって顧客に即座に提供されていますか?	イト http://aws.amazon.com を参照してください。
インフラストラクチャと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 規格に合わせて、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 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
インフラストラクチャと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 規格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 認証規格へ
	IVS-04.2	ハイパーバイザー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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	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、および予測される必要な容量を考慮に入れていますか?	の対応を確認する独立監査人から、審査および認証を受けています。
	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と仮想化セキュリティ 管理 – 脆弱性管理	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?	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、内部および外部のペネトレーション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。 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。
インフラストラクチャと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、複数のホワイトペーパー (http://aws.amazon.com/documentation/ で入手可能) 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。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	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?	ルールセット、アクセスコントロールリスト (ACL)、およびコンフィグレーションを採用する境界保護デバイスはネットワークファブリック間のデータフローを強化します。 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データフローを制御するデバイスによって分離されています。ファブリック間のデータフローは、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認証機能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データフローを制御します。ACL は適切な従業員が定義、承認し、AWS ACL 管理ツールを使用して管理、デプロイされます。 Amazon の情報セキュリティチームがこれらの ACL を承認します。ネットワークファブリック間の承認されたファイアウォールルールセットとアクセスコントロールリストが、データフロー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 時間ごとに）境界保護デバイス
	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、適切性を定期的にレビューしていますか?	
	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に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と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、ビジネスニーズを充足するために必要なポート、プロトコル、サービスだけを提供していますか?	に自動的にプッシュされて、ルールセットとアクセスコントロールリストが最新であることが確認されます。 AWS ネットワーク管理は、SOC、PCI DSS、ISO 27001、および FedRAMPsm への AWS の継続的な準拠の一環として、サードパーティーの独立監査人によって定期的に確認されます。 AWS は、そのインフラストラクチャコンポーネントを通じて最小権限を実装しています。また、特定のビジネス目的がないすべてのポートとプロトコルを禁止しています。AWS は、デバイスの使用に不可欠な機能のみの最小実装という厳格な手法に従っています。ネットワークスキャンを実行し、不要なポートまたはプロトコルが使用されている場合は修正されます。 AWS 環境内のホストオペレーティングシステム、ウェブアプリケーション、およびデータベースでさまざまなツールを利用した、定期的な内外部の脆弱性のスキャンが実行されます。脆弱性のスキャンと解決手法は、AWS の PCI DSS および FedRAMP への継続的な準拠の一環として定期的に確認されます。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
インフラストラクチャと仮想化セキュリティ 本番環境および非本番環境	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、本番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 の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、適切な本番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	本番環境および非本番環境を論理的および物理的に分離していますか?	AWS のお客様は、お客様が定義した要件に従って、お客様のネットワークセグメントを管理する責任を有します。 AWS 内部では、AWS のネットワークセグメントは ISO 27001 規格に合わせて構築されています。詳細については、ISO 27001 規格の附属書 A ドメイン 13 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
インフラストラクチャと仮想化セキュリティ セグメント化	IVS-09.1	ビジネスおよび顧客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?	
	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	本番環境と非本番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と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、本番用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、お客様が本番環境および非本番環境を保守および開発できるようにしています。運用データが非本番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。

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と仮想化セキュリティ VMM セキュリティ – ハイパーバイザー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。
インフラストラクチャと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 の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)?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	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と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 規格に合わせて構築されています。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。

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	技術的な措置を導入して、多層防御技術 (パケットの詳細分析、トラフィック制御、ブラックホーリングなど) を適用し、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を検知し、速やかに対処していますか?	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、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実施されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。 また、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。 AWS の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。
相互運用性とポータビリティ *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?	AWS API の詳細については、https://aws.amazon.com/documentation/ を参照してください。 AWS は、ISO 27001 規格に合わせて、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式なポリシー、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
相互運用性とポータビリティ 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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
相互運用性とポータビリティ ポリシーと法務	IPY-03.1	顧客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?	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 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。
	IPY-03.2	顧客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?	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。
相互運用性とポータビリティ 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できるようにしています。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、顧客 (テナント) に提供していますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
相互運用性とポータビリティ 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、内部および外部のペネトレーション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、ハイパーバイザーは、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、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。
	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、顧客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 規格に合わせています。詳細情報については、ISO 27001 規格の附属書 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確立し、ISO 27002 の管理策、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

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 承認済みアプリケーション	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?	報システム向けの推奨セキュリティ管理) に基づいて ISO 27001 認証フレームワークを効果的に統合しています。 お客様のデータと関連するメディア資産に対する統制と責任はお客様にあります。お客様には、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 *BYOD* 用承認済みソフトウェア	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ストアを明示していますか?	
モバイルセキュリティ 意識とトレーニング	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 クラウドベースのサービス	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?	

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?	
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?	

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 暗号化	MOS-11	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、デバイス全体もしくは機密情報として指定されたデータに対して、技術的制御手段により強制可能な暗号の使用を義務づけていますか?	
モバイルセキュリティ ジェイルブレイクおよびルート化	MOS-12.1	顧客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制御を回避することを禁止していますか (ジェイルブレイクやルート化など)?	
	MOS-12.2	組み込まれたセキュリティ制御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 法務関連	MOS-13.1	顧客の BYOD ポリシーでは、プライバシーに関する期待、および訴訟、E ディスカバリ、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。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	MOS-13.2	組み込まれたセキュリティ制御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	顧客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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	MOS-16.3	顧客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?	
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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	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?	
モバイルセキュリティ ユーザー	MOS-20.1	顧客の 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	顧客の 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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
セキュリティインシデント管理、E ディスカバリ、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?	AWS は、ISO 27001 規格の要件に従い、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。 AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
セキュリティインシデント管理、E ディスカバリ、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インシデント対応計画がありますか?	AWS のインシデント対応プログラム、計画、および手続きは、ISO 27001 規格に合わせて作成されています。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。 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。AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。 詳細については、AWS クラウドセキュリティホワイトペーパー
	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インシデント対応計画に統合していますか?	
	SEF-02.3	セキュリティインシデント時の自社とテナントの責任内容を示した役割と責任の文書を発行していますか?	
	SEF-02.4	過去 1 年間にセキュリティインシデント対応計画をテストしたことがありますか?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
セキュリティインシデント管理、E ディスカバリ、およびクラウドフォレンジック インシデントレポート	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?	(http://aws.amazon.com/security で入手可能) を参照してください。
	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インシデントを分離できますか?	
セキュリティインシデント管理、E ディスカバリ、およびクラウドフォレンジック インシデント対応の法的準備	SEF-04.1	インシデント対応計画は、法的に許容可能な保管の継続性の管理プロセスおよび統制の業界標準に準拠していますか?	
	SEF-04.2	インシデント対応機能には、法的に許容可能なフォレンジック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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	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?	
セキュリティインシデント管理、E ディスカバリ、およびクラウドフォレンジック インシデント対応のメトリクス	SEF-05.1	すべての情報セキュリティインシデントの種類、規模、および影響を監視および数値化していますか?	AWS セキュリティメトリクスは、ISO 27001 規格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 規格の附属書 A ドメイン 16 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
	SEF-05.2	依頼に応じて、統計的な情報セキュリティインシデント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。
	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?	

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 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、関係する顧客やプロバイダーに対してセキュリティインシデント情報を定期的に提供していますか?	AWS のインシデント対応プログラム、計画、および手続きは、ISO 27001 規格に合わせて作成されています。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 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 規格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 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
	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	顧客のポリシー、手順、およびサポート対象の対策とメトリ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 サプライヤーとの関係を維持しています。 詳細については、ISO 27001 規格の附属書 A、ドメイン 15 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
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?	
	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。

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 サプライチェーンメトリクス	STA-07.1	プロバイダーおよび顧客 (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?	
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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	STA-8.2	毎年のレビューには、顧客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 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 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	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 規格に合わせています。詳細については、AWS SOC レポートを参照してください。

統制グループ	CID	コンセンサス評価の質問	AWS の回答
あるソフトウェア対策	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?	また、詳細については、ISO 27001 規格の附属書 A ドメイン 12 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
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実行していますか?	お客様は、自身のゲストオペレーティングシステム、ソフトウェア、アプリケーションの統制を有しており、脆弱性スキャンを実行し、お客様のシステムにパッチを適用するのは、お客様の責任です。対象をお客様のインスタンスに限定し、かつ AWS 利用規約に違反しない限り、お客様はご自身のクラウドインフラストラクチャのスキャンを実施する許可をリクエストできます。AWS セキュリティは、すべてのインターネット向きサービスエンドポイントの IP アドレスの脆弱性を定期的にスキャンしています。判明した脆弱性があれば、修正するために適切な関係者に通知します。通常、AWS の保守およびシステムのパッチ適用はお客様に影響がありません。
	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実行していますか?	
	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実行していますか?	
	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?	

統制グループ	CID	コンセンサス評価の質問	AWS の回答
	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?	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。また、ISO 27001 規格の附属書 A ドメイン 12 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。
	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について、実行を禁止していますか?	

詳細情報

詳細については、以下のソースを参照してください。

- AWS リスクとコンプライアンスの概要
- AWS の認証、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
- 主要なコンプライアンスに関する質問と AWS の回答

ドキュメントの改訂

変更	説明
2017 年 9 月	日本語版発行
2017 年 1 月	新フォーマットに移行
2016 年 1 月	英語初版発行