「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実1	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実2	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実3	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実4	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実5	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実6	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実7	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実8	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実9	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実10	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実11	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実12	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実13	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実14	○	○	・AWSネットワークは、従来のネットワークセキュリティ問題に対する強力な保護機能を提供します。 保護機能の例： - 分散サービス拒否（DDoS）攻撃 - 中間者（MITM）による攻撃 - IPスプーフィング - ポートスキャン - 第三者によるパケットスニッフィング AWS は、様々な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。AWS モニタリングツールは、異常な、または不正なアクティビティと条件を通信の出入り口で検出するように設計されています。これらのツールは、サーバーおよびネットワークの利用状況、ポートスキャニングアクティビティ、アプリケーションの利用状況、および許可されていない侵入の試みをモニタリングします。 モニタリングに加えて、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様々なツールを使用した脆弱性のスキャンが定期的に実行されます。また、AWS セキュリティチームは、該当するベンダーの不具合に関するニュースフィードを購読し、積極的にベンダーのウェブサイトやその他の関連する販売経路を監視し、新しいパッチがないかどうかの確認を行っています。さらに、AWS のお客様から各種問題を AWS にご報告いただけるようにしています。AWS 脆弱性レポートのウェブサイト（http://aws.amazon.com/security/vulnerability-reporting/）をご利用ください	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 インフラストラクチャ保護: Amazon Virtual Private Cloud (Amazon VPC) を使用して、お客様が定義した仮想ネットワーク内で AWS リソースを起動できます。Amazon CloudFront は、DDoS を緩和する AWS Shield に統合されたビューワーに対して、データ、動画、アプリケーション、API を安全に提供する、グローバルコンテンツ配信ネットワークです。AWS WAF は、ウェブの一般的な脆弱性からウェブアプリケーションを保護するために役立つ、Amazon CloudFront または Application Load Balancer にデプロイされたウェブアプリケーションファイアウォールです。	アマゾン ウェブ サービス ： セキュリティプロセスの概要
実15	○	○	・AWS では、インバウンドとアウトバウンドの通信およびネットワークトラフィックをより包括的に監視することを考え、限られた数のクラウドへのアクセスポイントを戦略的に設置しました。このようなお客様のアクセスポイントは API エンドポイントと呼ばれ、安全な HTTP アクセス（HTTPS）を許可します。これにより、ご利用のストレージまたは AWS 内のコンピューティングインスタンスとの安全な通信セッションを確立できます。FIPS 暗号要件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 終端ロードバランサーは、FIPS 140-2 に準拠しています。 さらに、AWS は、インターネットサービスプロバイダ（ISP）とのインターフェイス通信を管理するためのネットワークデバイスを実装しました。AWS ネットワークのインターネット側のそれぞれの境界では、複数の通信サービスへの重複する接続を採用しています。これらの接続にはそれぞれ、専用ネットワークデバイスがあります。 追加情報については、"アマゾン ウェブ サービス: セキュリティプロセスの概要"を参照してください。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 お客様はAmazon VPCを使用することにより、アマゾン ウェブ サービス (AWS) クラウド内で論理的に分離したセクションをプロビジョニングし、お客様が定義する仮想ネットワークで AWS リソースを起動できます。また、VPC 内のセキュリティグループにより、各 Amazon EC2 インスタンスにおける着信および発信両方のネットワークトラフィックを指定することができます。明示的に許可されていないトラフィックは自動的に拒否されます。 セキュリティグループに加えて、各サブネットに出入りするネットワークトラフィックは、ネットワークアクセスコントロールリスト (ACL) を使用して許可または拒否することができます。 AWS PrivateLink を使用して、VPC と AWS のサービスをセキュアでスケーラブルな方法で接続できます。AWS PrivateLink のトラフィックはインターネットを経由しないため、ブルートフォース攻撃や DDoS (分散型サービス拒否) 攻撃の脅威に晒される危険を軽減できます。プライベート IP 接続とセキュリティグループを使用することで、サービスは自社のプライベートネットワークで直接ホストしているように機能します。	アマゾン ウェブ サービス ： セキュリティプロセスの概要

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実16	○	○	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/IEC 27001、および FedRAMPsm 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。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 AWS Shield は、AWS で実行されるアプリケーションを Distributed Denial of Service (DDoS) 攻撃から保護するマネージド型のサービスです。AWS Shield Standard は、すべてのお客様に対し追加料金なしで自動的に有効化されます。AWS Shield Advanced は任意で利用できる有料サービスです。AWS Shield Advanced により、Amazon EC2、Elastic Load Balancing (ELB)、Amazon CloudFront、AWS Global Accelerator、Route 53 で実行中のアプリケーションを標的とする、高度化された大規模な攻撃からの保護を強化することができます。 また、Amazon GuardDuty は、AWS アカウントとワークロードを継続的にモニタリングおよび保護できる脅威検出機能を提供しています。お客様はGuardDuty を使用することで、AWS CloudTrail イベント、Amazon VPC フローログ、および DNS ログで見つかったアカウントとネットワークアクティビティから生成されたメタデータの連続ストリームを分析することができます。また、既知の悪意のある IP アドレス、異常の検出、機械学習などの統合された脅威インテリジェンスを使用して、脅威をより正確に識別することができます。	アマゾン ウェブ サービス：リスクとコンプライアンス
実17	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実18	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実19	○	○	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/IEC 27001 の認証基準に合わせて作成されています。AWS SOC 1 Type 2 レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。 詳細については、”アマゾン ウェブ サービス：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。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 お客様はAmazon Detective を使用することにより、潜在的なセキュリティ問題や不審なアクティビティの根本原因を簡単に分析、調査し、すばやく特定できます。Amazon Detective は、AWS リソースからログデータを自動的に収集し、機械学習、統計的分析、グラフ理論を使用して、リンクされたデータセットを構築します。これにより、より迅速かつ効率的なセキュリティ調査を簡単に行えます。	アマゾン ウェブ サービス：セキュリティプロセスの概要
実20	○	○	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/IEC 27001 に準拠しています。 詳細についてはISO/IEC 27001 の附属書 A、ドメイン 12 を参照してください。AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 また、Amazon の資産 (ノートパソコンなど) は、E メールのフィルタリングとマルウェア検出を含むウイルス対策ソフトウェアで設定されています。 AWS ネットワークファイアウォール管理および Amazon のウイルス対策プログラムは、SOC、PCI DSS、ISO/IEC 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。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実21	○	○	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/IEC 27001 に準拠しています。 詳細についてはISO/IEC 27001 の附属書 A、ドメイン 12 を参照してください。AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 また、Amazon の資産 (ノートパソコンなど) は、E メールのフィルタリングとマルウェア検出を含むウイルス対策ソフトウェアで設定されています。 AWS ネットワークファイアウォール管理および Amazon のウイルス対策プログラムは、SOC、PCI DSS、ISO/IEC 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。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	アマゾン ウェブ サービス：リスクとコンプライアンス
実22	○	○	AWS の事故対応プログラム、計画、および手続きは、ISO/IEC 27001 に準拠し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	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	・AWS CSA Consensus Assessments Initiative Questionnaire (CAIQ) ・アマゾン ウェブ サービス：リスクとコンプライアンス
実23	○	○	AWS セキュリティフレームワークは、NIST SP800-53、ISO/IEC 27001、ISO/IEC 27017、ISO/IEC 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 、アマゾン ウェブ サービス ：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。 AWS には、毎年（またはポリシーに影響するシステムへの大きな変更が発生したときに）確認、更新される正式なアクセスコントロールポリシーがあります。このポリシーでは、目的、範囲、役割、責任、および管理コミットメントについて取り上げています。AWS は最小権限という概念を導入しており、ユーザーがジョブ機能を実行するために必要最小限のアクセスを許可しています。ユーザーアカウントの作成では、最小アクセス権を持つユーザーアカウントが作成されます。これらの最小権限を超えるアクセスには、適切な認証が必要になります。詳細情報については、ISO/IEC 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/IEC 27001 および ISO/IEC 27018 に準拠している旨の審査と認定を受けています。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	アマゾン ウェブ サービス：セキュリティプロセスの概要 アマゾン ウェブ サービス：リスクとコンプライアンス
実24	○	○	AWS のビジネス継続性ポリシーおよび計画は、ISO/IEC 27001 に準拠して開発され、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/IEC 27001 の附属書 A、ドメイン 17を参照してください。 詳細については 、アマゾン ウェブ サービス ：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。 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。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	AWS CSA Consensus Assessments Initiative Questionnaire (CAIQ) アマゾン ウェブ サービス：リスクとコンプライアンス

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実25	○	○	AWS は、ISO/IEC 27001 に準拠して、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 、アマゾン ウェブ サービス ：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。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 お客様はAWS Identity and access Management(IAM) を使用して、お客様の AWS リソースへの個人またはグループによるアクセスを安全にコントロールすることができます。 お客様はCloudTrail を使用することで、リクエストを実行したユーザー、使用したサービス、実行されたアクション、そのアクションのパラメーター、AWS のサービスによって返されたレスポンス要素など、各アクションの重要な情報が記録することができます。この情報は、AWS リソースに加えられた変更を追跡し、操作に関する問題を解決するために役立ちます。	アマゾン ウェブ サービス：リスクとコンプライアンス
実26	○	○	AWSではISO/IEC 27001およびPCI DSSに則り、AWSリソースへの論理的なアクセスのために必要なパスワードポリシーを定めています。パスワードは複雑である必要があり、90 日おきに変更されます。 AWS環境におけるパスワード要件の詳細については、PCI DSS レポート 8.2 および SOC2 タイプ2レポートを参照ください。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 お客様はAWS Identity and access Management(IAM) を使用して、お客様の AWS リソースへの個人またはグループによるアクセスを安全にコントロールすることができます。AWS IAMでは、パスワードの最小長を定義したり、数字を 1 つ以上含めるようにするなど、強力なパスワードを要求できます。自動パスワード失効の実施、以前に使用したパスワードの再利用禁止、次回 AWS サインイン時のパスワードリセットの要求も設定できます	PCI DSS 8.2.3 PCI DSS 8.2.4
実27	○	○	AWS 本稼働環境のネットワークは、Amazon 社内ネットワークから分離されており、論理的アクセスのために個別の認証情報が必要です。 AWS クラウドのコンポーネントにアクセスする必要がある Amazon 社内ネットワーク上の AWS 開発者と管理者は、AWS アクセス管理システムを通して明示的にアクセスをリクエストしなければなりません。すべてのリクエストは、適切な所有者または管理者によって確認および承認されます。 アカウントの確認および監査 アカウントは 90 日ごとにレビューされます。明示的な再承認が必要となり、これを行わない場合は、リソースに対するアクセス権が自動的に取り消されます。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。Windows および UNIX のアカウントは無効となり、Amazon の権限管理システムは全システムからそのユーザーを削除します。 アクセスに関する変更リクエストは、Amazon 権限管理ツールの監査ログに記録されます。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。承認しない場合、アクセス権は自動的に取り消されます。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	アマゾン ウェブ サービス – セキュリティプロセスの概要
実28	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実29	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実30	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実31	○	○	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。 ISO/IEC 27001 に準拠して、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。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	アマゾン ウェブ サービス ： セキュリティプロセスの概要 アマゾン ウェブ サービス：リスクとコンプライアンス
実32	○	○	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/IEC 27001に準拠しています。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/IEC 27001 の附属書 A、ドメイン 12 を参照してください。AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 また、Amazon の資産 (ノートパソコンなど) は、E メールのフィルタリングとマルウェア検出を含むウイルス対策ソフトウェアで設定されています。 AWS ネットワークファイアウォール管理および Amazon のウイルス対策プログラムは、SOC、PCI DSS、ISO/IEC 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。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	アマゾン ウェブ サービス：リスクとコンプライアンス
実33	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実34	○	○	AWS ネットワーク管理は、SOC、PCI DSS、ISO/IEC 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。 ネットワークの監視と保護 AWS は、様々な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。AWS モニタリングツールは、異常な、または不正なアクティビティと条件を通信の出入り口で検出するように設計されています。これらのツールは、サーバーおよびネットワークの利用状況、ポートスキャニングアクティビティ、アプリケーションの利用状況、および許可されていない侵入の試みをモニタリングします。このツールを使用して、異常なアクティビティに対して独自に性能測定基準のしきい値を設定することができます。 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。主要なオペレーションメトリックが早期警告しきい値を超えた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（常時待機体制）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することができます。ポケットベルシステムがサポートされ、アラームが迅速かつ確実に運用担当者に届きます。 AWS 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様々なツールを使用した脆弱性のスキャンが定期的に実行されます。また、AWS セキュリティチームは、該当するベンダーの不具合に関するニュースフィードを購読し、積極的にベンダーのウェブサイトやその他の関連する販売経路を監視し、新しいパッチがないかどうかの確認を行っています。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	アマゾン ウェブ サービス：リスクとコンプライアンス アマゾン ウェブ サービス ： セキュリティプロセスの概要
実35	○	○	AWSではAWS 人事管理システムのオンボーディングワークフロープロセスの一環として、一意のユーザー ID が作成されます。デバイスプロビジョニングプロセスは、デバイスの ID を確実に一意にするうえで役立ちます。両方のプロセスとも、ユーザーアカウントまたはデバイスを確立するためのマネージャーの承認が含まれます。最初の認証は、プロビジョニングプロセスの一部としてユーザーに対面で提供されるとともに、デバイスにも提供されます。内部ユーザーは SSH パブリックキーをアカウントに関連付けることができます。システムカウントの認証は、リクエスタの ID を確認した後で、アカウント作成プロセスの一部としてリクエスタに提供されます。 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。 AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO/IEC 27001、およびFedRAMPsm 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	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	アマゾン ウェブ サービス：リスクとコンプライアンス アマゾン ウェブ サービス：セキュリティプロセスの概要 AWS データセンターWebサイト：境界防御レイヤー https://aws.amazon.com/jp/compliance/data-center/perimeter-layer/

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実36	○	○	AWS は、変更の管理にシステム的なアプローチを採用しています。そのためお客様に影響を与えるサービスの変更は、徹底的に検証、テスト、承認され、充分な情報が提供されます。変更の実稼動環境への投入は通常、最も影響の小さいエリアへの段階的配備から開始されます。デプロイは単一のシステムでテストされ、影響が評価できるよう綿密にモニタリングされます。 AWS変更管理アプローチでは、変更が本番環境にデプロイされる前に、次の手順を完了する必要があります。 1.適切なAWS変更管理ツールを通じて変更を文書化し、伝達します。 2.混乱を最小限に抑えるために、変更およびロールバック手順の実装を計画します。 3.論理的に分離された非運用環境で変更をテストします。 4.ビジネスへの影響と厳密な技術に重点を置いて、変更のピアレビューを完了します。レビューにはコードレビューを含める必要があります。 5.権限のある者による変更の承認を得 ます。 社員が個々の役割と責任を理解するのを助けるため、ISO/IEC 27001に準拠した、完了確認を必要とする定期的な情報セキュリティトレーニングを実施しています。従業員が確立されたポリシーを理解し、従っているかについてはコンプライアンス監査が定期的に行われます。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	AWS CSA Consensus Assessments Initiative Questionnaire (CAIQ) アマゾン ウェブ サービス：リスクとコンプライアンス アマゾン ウェブ サービス：セキュリティプロセスの概要
実37	○	○	AWS は、変更の管理にシステム的なアプローチを採用しています。そのためお客様に影響を与えるサービスの変更は、徹底的に検証、テスト、承認され、充分な情報が提供されます。変更の実稼動環境への投入は通常、最も影響の小さいエリアへの段階的配備から開始されます。デプロイは単一のシステムでテストされ、影響が評価できるよう綿密にモニタリングされます。 可能な場合、変更は通常の変更時間帯に予定されます。標準の変更管理手順と異なる手順を必要とする実稼動システムに対する緊急の変更は、インシデントと関連付けられており、必要に応じて記録され、承認されます。 AWS は、重要なサービスの変更に対する自己監査を定期的に行っており、品質をモニタリングしながら高い基準を維持することによって、変更管理プロセスの継続的な改善に貢献しています。例外は分析され、根本的な原因が決定さ れて適切な措置が取られます。変更はコンプライアンスに従うようにされるか、または必要に応じてロールバックされます。その後プロセスまたは人的問題を解決して修正するための措置が取られます。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	アマゾン ウェブ サービス：セキュリティプロセスの概要
実38	○	○	すべてのアクティビティはセキュリティレビューのために記録されます。また、AWS 従業員によるデータセンターへのすべての物理的アクセスは記録され、定期的に監査されます	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	アマゾン ウェブ サービス：セキュリティプロセスの概要
実39	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実40	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実41	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

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。

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実42	○	○	AWS は、変更の管理にシステム的なアプローチを採用しています。そのためお客様に影響を与えるサービスの変更は、徹底的に検証、テスト、承認され、充分な情報が提供されます。AWS の変更管理プロセスは、意図しないサービス障害を防ぎ、お客様に対するサービスの完全性を維持することを目的としています。AWS は、重要なサービスの変更に対する自己監査を定期的に行っており、品質をモニタリングしながら高い基準を維持することによって、変更管理プロセスの継続的な改善に貢献しています。例外は分析され、根本的な原因が決定されて適切な措置が取られます。変更はコンプライアンスに従うようにされるか、または必要に応じてロールバックされます。その後プロセスまたは人的問題を解決して修正するための措置が取られます。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 お客様はAWSリソースの管理にAWS Configを使用することができます。AWS Config は、セキュリティとガバナンスのためのフルマネージド型のサービスであり、ご利用の AWS リソースのインベントリ、構成履歴、構成変更通知の機能を備えています。AWS Config では、既存の AWS リソースの特定や、構成の詳細すべてを含めたお客様の AWS リソースインベントリのエクスポートが可能になり、特定の時点でどのようにリソースが構成されたかを判断できます。これらの機能は、コンプライアンス監査、セキュリティ分析、リソース変更の追跡、トラブルシューティングを可能にします。	アマゾン ウェブ サービス：セキュリティプロセスの概要
実43	○	○	内部的には、AWSネットワークセグメンテーションはISO/IEC 27001に準拠しています。詳細については、ISO/IEC 27001の附属書A.ドメイン13を参照してください。 AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 AWS は、変更の管理にシステム的なアプローチを採用しています。そのためお客様に影響を与えるサービスの変更は、徹底的に検証、テスト、承認され、充分な情報が提供されます。AWS の変更管理プロセスは、意図しないサービス障害を防ぎ、お客様に対するサービスの完全性を維持することを目的としています。実稼働環境にデプロイされる変更には、以下の対応が行われます: - 検証: 変更の技術的側面について専門家による検証が必要です。 - テスト: 適用されている変更は、予想どおりに動作し、パフォーマンスに悪影響を与えないことを確認するためにテストされます。 - 承認: すべての変更は、ビジネスへの影響を適切に監視し、それらの影響についての情報を提供するために、承認される必要があります。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 お客様はAWSリソースの管理にAWS Configを使用することができます。AWS Config は、セキュリティとガバナンスのためのフルマネージド型のサービスであり、ご利用の AWS リソースのインベントリ、構成履歴、構成変更通知の機能を備えています。AWS Config では、既存の AWS リソースの特定や、構成の詳細すべてを含めたお客様の AWS リソースインベントリのエクスポートが可能になり、特定の時点でどのようにリソースが構成されたかを判断できます。これらの機能は、コンプライアンス監査、セキュリティ分析、リソース変更の追跡、トラブルシューティングを可能にします。	アマゾン ウェブ サービス：セキュリティプロセスの概要
実44	○	○	AWS は、AWS 製品の設計、開発、運用において、優れた商用 IT プラクティスを確実に活用する責任があります。 AWS は、お客様の信頼と信頼の維持を最も重要視しているため、可用性、完全性、機密性の観点から AWS 製品の品質属性を定義します。 AWS 品質システムは、組織構造、責任、手順、プロセス、リソースなど、AWS が品質管理を実装するために必要な要素に対応します。 AWS は、国際標準化機構（ISO）によって確立されたベストプラクティスガイドラインを満たす、またはそれ以上の品質管理システムを確立しています。 品質管理システムは、AWS サービス、AWS インフラストラクチャ、AWS サービスの開発と運用をサポートするアセットを含む AWS 製品の開発と運用に適用されます。 品質マネジメントシステムに適用される主要な規格には、ISO 9001、ISO/IEC 27001、ISO/IEC 27017、ISO/IEC 27018 があります。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	アマゾン ウェブ サービス：リスクとコンプライアンス
実45	○	○	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/IEC 27001 に準拠しています。AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 詳細については、”アマゾン ウェブ サービス :セキュリティプロセスの概要 ”ホワイトペ～パー(http://aws.amazon.com/security で入手可能) を参照してください。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	アマゾン ウェブ サービス：リスクとコンプライアンス

「対応の主体」凡例　○ ：主体として対応する
-　：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実46	○	○	AWS モニタリングツールは、異常な、または不正なアクティビティと条件を通信の出入り口で検出するように設計されています。これらのツールは、サーバーおよびネットワークの利用状況、ポートスキャニングアクティビティ、アプリケーションの利用状況、および許可されていない侵入の試みをモニタリングします。このツールを使用して、異常なアクティビティに対して独自に性能測定基準のしきい値を設定することができます。 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。主要なオペレーションメトリックが早期警告しきい値を超えた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（常時待機体制）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することができます。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 AWS Cloudwatchは、AWSのクラウド資源及びお客様が運用するアプリケーションに対するモニタリングを提供しま す。また、AWSはサービス提供の最新の状況をAWS Service Health Dashboard(https://status.aws.amazon.com/)にて公開しています。	アマゾン ウェブ サービス：セキュリティプロセスの概要
実47	○	○	AWS モニタリングツールは、異常な、または不正なアクティビティと条件を通信の出入り口で検出するように設計されています。これらのツールは、サーバーおよびネットワークの利用状況、ポートスキャニングアクティビティ、アプリケーションの利用状況、および許可されていない侵入の試みをモニタリングします。このツールを使用して、異常なアクティビティに対して独自に性能測定基準のしきい値を設定することができます。 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。主要なオペレーションメトリックが早期警告しきい値を超えた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（常時待機体制）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することができます。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 AWS Cloudwatchは、AWSのクラウド資源及びお客様が運用するアプリケーションに対するモニタリングを提供しま す。 また、AWSはサービス提供の最新の状況をAWS Service Health Dashboard(https://status.aws.amazon.com/)にて公開しています。	AWS Webサイト：AWSのコントロール - セキュアな設定 https://aws.amazon.com/jp/compliance/data-center/controls/
実48	○	○	AWSはISO/IEC 27001 に準拠して、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。 追加の詳細については、ISO/IEC 27001の附属書 A. 8を参照してください。AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 AWS Systems Manager を使用することで、複数の AWS のサービスの運用データを一元化し、AWS リソース全体のタスクを自動化できます。アプリケーション、アプリケーションスタックのさまざまなレイヤー、本番環境と開発環境といったリソースの論理グループを作成できます。Systems Manager では、リソースグループを選択し、その最新の API アクティビティ、リソース設定の変更、関連する通知、運用アラート、ソフトウェアインベントリ、パッチコンプライアンス状況を表示できます。運用ニーズに応じて、各リソースグループに対してアクションを実行することもできます。Systems Manager により、AWS リソースを一元的に表示および管理でき、運用を完全に可視化して制御できます。	アマゾン ウェブ サービス ：リスクとコンプライアンス AWS Systems Manager のよくある質問 https://aws.amazon.com/jp/systems-manager/faq/

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。

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実49	○	-	・AWSはISO/IEC 27001 に準拠して、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。 追加の詳細については、ISO/IEC 27001の附属書 A. 11を参照してください。AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 ・AWS のデータセンターは、外部からはそれとはわからないようになっています。ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。 ・AWS は、権限を持つ担当者のみにデータセンターへの物理的なアクセスを許可しています。データセンターへのアクセスを必要とするすべての担当者は、まずアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最少権限の原則に基づき許可されますが、個人がアクセスを必要とするデータセンターのレイヤーを指定する必要があり、アクセスの期限が設定されます。申請は権限を持つ人物のみが審査して承認し、請求した期限が過ぎた後は、アクセスが取り消されます。入場を許可された担当者は、その権限で指定されたエリアのみに入場が制限されます。	-	アマゾン ウェブ サービス：リスクとコンプライアンス アマゾン ウェブ サービス：セキュリティプロセスの概要 AWS Webサイト：AWSのコントロール - セキュアな設定 https://aws.amazon.com/jp/compliance/data-center/controls/
実50	○	-	・AWSはISO/IEC 27001 に準拠して、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。 追加の詳細については、ISO/IEC 27001の附属書 A. 8を参照してください。AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 ・AWS のデータセンターは、外部からはそれとはわからないようになっています。ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。 ・AWS は、権限を持つ担当者のみにデータセンターへの物理的なアクセスを許可しています。データセンターへのアクセスを必要とするすべての担当者は、まずアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最少権限の原則に基づき許可されますが、個人がアクセスを必要とするデータセンターのレイヤーを指定する必要があり、アクセスの期限が設定されます。申請は権限を持つ人物のみが審査して承認し、請求した期限が過ぎた後は、アクセスが取り消されます。入場を許可された担当者は、その権限で指定されたエリアのみに入場が制限されます。	-	アマゾン ウェブ サービス :リスクとコンプライアンス アマゾン ウェブ サービス :セキュリティプロセスの概要
実51	○	-	・AWS は電気および機械に関連する設備をモニタリングし、予防的なメンテナンスを実施して、AWS データセンター内のシステムの継続的な運用性を維持しています。機器のメンテナンス手順は資格を持っている担当者が実行し、文書化されたメンテナンススケジュールに従って完了されます。 ・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。 ・In order to ensure maintenance procedures are properly executed, AWS assets are assigned an owner, tracked and monitored with AWS proprietary inventory management tools. AWS asset owner procedures are carried out by method of utilizing a proprietary tool with specified checks that must be completed according to the documented maintenance schedule. Third party auditors test AWS equipment maintenance controls by validating that the asset owner is documented and that the condition of the assets are visually inspected according to the documented maintenance policy. （参考訳）保守作業が適切に実施されていることを検証するために、AWS専用インベントリ管理ツールを使用して、AWSのアセットに所有者を割り当て、追跡および監視を行っています。文書化された保守スケジュールに沿って検証が実施できるように、専用ツールを使ってAWSアセット所有者の作業を管理しています。独立した監査人はAWSの機器の保守に対する統制を検証しています。この検証ではアセットに所有者が割り当てられ、文書化された保守作業のポリシーに従ってアセットの状態が目視で検証されていることをチェックします。	-	AWS Webサイト - コントロール https://aws.amazon.com/jp/compliance/data-center/controls/ アマゾン ウェブ サービス :リスクとコンプライアンス AWS CSA Consensus Assessments Initiative Questionnaire (CAIQ) Feburary, 2020

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実52	○	-	AWS は電気および機械に関連する設備をモニタリングし、予防的なメンテナンスを実施して、AWS データセンター内のシステムの継続的な運用性を維持しています。 機器のメンテナンス手順は資格を持っている担当者が実行し、文書化されたメンテナンススケジュールに従って完了されます。	-	AWS Webサイト：コントロール https://aws.amazon.com/jp/compliance/data-center/controls/
実53	○	-	・AWSはISO/IEC 27001 に準拠して、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。追加の詳細については、ISO/IEC 27001の附属書 A. 8を参照してください。AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 ・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。 ・AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。 ・データセンターの電力システムは、完全に冗長性をもち、運用に影響を与えることなく管理が可能となっています。1日24時間体制で、年中無休で稼働しています。施設内で重要かつ不可欠な負荷に対応するために、電力障害時には無停電電源装置（UPS）がバックアップ電力を供給しています。データセンターは、発電機を使用して施設全体のバックアップ電力を供給しています。 ・サーバーその他のハードウェアの運用温度を一定に保つために、空調制御が必要です。これによって過熱を防ぎ、サーバー停止の可能性を減らすことができます。データセンターは、大気の状態を最適なレベルに保つように設定されています。作業員とシステムが、温度と湿度を適切なレベルになるように監視してコントロールしています。	-	アマゾン ウェブ サービス：リスクとコンプライアンス AWS Webサイト：データセンター - AWSのコントロール https://aws.amazon.com/jp/compliance/data-center/controls/ アマゾン ウェブ サービス：セキュリティプロセスの概要
実54	○	-	AWS は、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/IEC 27001 認証を取得しています。 AWS は電気および機械に関連する設備をモニタリングし、予防的なメンテナンスを実施して、AWS データセンター内のシステムの継続的な運用性を維持しています。 機器のメンテナンス手順は資格を持っている担当者が実行し、文書化されたメンテナンススケジュールに従って完了されます。 また、問題の速やかな特定を可能にするため、電気的、機械的なシステムおよび設備をモニタリングしています。これは継続的な監査ツールと、建物管理および電気的なモニタリングシステムを通じて提供される情報を利用して行われます。予防的メンテナンスが実行され、設備の運用に関しての継続性が保たれています。 データセンター環境の物理的な管理方法については、SOC1 Type2 reportの以下にも記載しております。 E. Physical Security and Environmental Protection ・Environment Management	-	AWS Webサイト：AWSのコントロール https://aws.amazon.com/jp/compliance/data-center/controls/ アマゾン ウェブ サービス: リスクとコンプライアンス ホワイトペーパー

「対応の主体」凡例　○：主体として対応する
-　：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実55	○	-	AWS は、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/IEC 27001 認証を取得しています。 Amazonのデータセンターは最新式で、革新的で建築的かつ工学的アプローチを採用しています。Amazon は大規模データセンターの設計、構築、運用において、長年の経験を有しています。この経験は、AWS プラットフォームとインフラストラクチャに活かされています。 データセンター設備は問題が速やかに特定されるように、電気、機械、ライフサポートシステムおよび設備を監視しています。予防的メンテナンスが実行され、設備を継続的な運用性が保たれています。 火災検出と鎮火 自動火災検出および鎮火装置が取り付けられ、リスクを軽減しています。この火災検出システムは、全データセンター環境、機械的及び電気的インフラストラクチャースペース、冷却室および発電機設備室において、煙検出センサーを使用しています。これらのエリアは、充水型、二重連結予作動式、またはガス式スプリンクラーシステムによって守られています。 電力 データセンターの電力システムは、完全に冗長性をもち、運用に影響を与えることなく管理が可能となっています。１日24時間体制で、年中無休で稼動しています。施設内で重要かつ不可欠な負荷に対応するために、電力障害時には無停電電源装置（UPS）がバックアップ電力を供給しています。データセンターは、発電機を使用して施設全体のバックアップ電力を供給しています。	-	アマゾン ウェブ サービス：セキュリティプロセスの概要

「対応の主体」凡例　○：主体として対応する
-　：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
			空調と温度 サーバーその他のハードウェアの運用温度を一定に保つために、空調制御が必要です。これによって過熱を防ぎ、サーバー停止の可能性を減らすことができます。データセンターは、大気の状態を最適なレベルに保つように設定されています。作業員とシステムが、温度と湿度を適切なレベルになるよう監視してコントロールしています。 物理的な環境保護の統制に対する監査レポートとして、SOC1 Type2 reportの以下にも記載しております。 ・Control Objective 5: Physical Security and Environmental Protection No7~No12		

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実56	○	-	AWS は、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/IEC 27001 認証を取得しています AWSのデータセンターでは、ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。 AWS は、権限を持つ担当者のみにデータセンターへの物理的なアクセスを許可しています。データセンターへのアクセスを必要とするすべての担当者は、まずアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最少権限の原則に基づき許可されますが、個人がアクセスを必要とするデータセンターのレイヤーを指定する必要があり、アクセスの期限が設定されます。申請は権限を持つ人物のみが審査して承認し、請求した期限が過ぎた後は、アクセスが取り消されます。入場を許可された担当者は、その権限で指定されたエリアのみに入場が制限されます。	-	アマゾン ウェブ サービス: リスクとコンプライアンス アマゾン ウェブ サービス : セキュリティプロセスの概要 AWS Webサイト : AWS のコントロール - 物理アクセス https://aws.amazon.com/jp/compliance/data-center/controls/#Physical_Access
実57	○	-	AWS は、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/IEC 27001 認証を取得しています AWSのデータセンターでは、ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。 AWS は、権限を持つ担当者のみにデータセンターへの物理的なアクセスを許可しています。データセンターへのアクセスを必要とするすべての担当者は、まずアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最少権限の原則に基づき許可されますが、個人がアクセスを必要とするデータセンターのレイヤーを指定する必要があり、アクセスの期限が設定されます。申請は権限を持つ人物のみが審査して承認し、請求した期限が過ぎた後は、アクセスが取り消されます。入場を許可された担当者は、その権限で指定されたエリアのみに入場が制限されます。 第三者のアクセスについては、承認された AWS の担当者が申請する必要があり、その担当者は第三者によるアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最少権限の原則に基づいて付与されます。申請では個人がアクセスを必要とするデータセンターのレイヤーを指定する必要があり、期限が設定されます。これらの申請は権限を持つ人物のみが審査して承認し、請求した期限が過ぎた後は、アクセスが取り消されます。入場を許可された担当者は、その権限で指定されたエリアのみ入場できます。訪問者バッジを与えられた担当者は、現場への到着後身分証明書を提示します。署名後に入場が許可され、権限を持つスタッフが常に付き添います。	-	アマゾン ウェブ サービス: リスクとコンプライアンス アマゾン ウェブ サービス : セキュリティプロセスの概要 AWS Webサイト : AWS のコントロール - 物理アクセス https://aws.amazon.com/jp/compliance/data-center/controls/#Physical_Access

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実58	○	-	AWS は、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/IEC 27001 認証を取得しています AWSのデータセンターでは、ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。 AWS は、権限を持つ担当者のみにデータセンターへの物理的なアクセスを許可しています。データセンターへのアクセスを必要とするすべての担当者は、まずアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最少権限の原則に基づき許可されますが、個人がアクセスを必要とするデータセンターのレイヤーを指定する必要があり、アクセスの期限が設定されます。申請は権限を持つ人物のみが審査して承認し、請求した期限が過ぎた後は、アクセスが取り消されます。入場を許可された担当者は、その権限で指定されたエリアのみに入場が制限されます。 第三者のアクセスについては、承認された AWS の担当者が申請する必要があり、その担当者は第三者によるアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最少権限の原則に基づいて付与されます。申請では個人がアクセスを必要とするデータセンターのレイヤーを指定する必要があり、期限が設定されます。これらの申請は権限を持つ人物のみが審査して承認し、請求した期限が過ぎた後は、アクセスが取り消されます。入場を許可された担当者は、その権限で指定されたエリアのみ入場できます。訪問者バッジを与えられた担当者は、現場への到着後身分証明書を提示します。署名後に入場が許可され、権限を持つスタッフが常に付き添います。	-	アマゾン ウェブ サービス: リスクとコンプライアンス アマゾン ウェブ サービス : セキュリティプロセスの概要 AWS Webサイト : AWS のコントロール - 物理アクセス https://aws.amazon.com/jp/compliance/data-center/controls/#Physical_Access
実59	○	-	セキュリティを保つべき領域での作業に関する管理策はISO/IEC 27001に規定されており、AWSのデータセンターにおける運用管理策についてはISO/IEC 27001認証を取得しています。詳細については ISO/IEC 27001 の附属書 A.11.1.5 をご参照ください。 すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。AWS は、そのような権限に対して正規のビジネスニーズがある従業員や業者に対してのみデータセンターへのアクセスや情報を提供しています。従業員がこれらの特権を必要とする作業を完了すると、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 データセンターへの物理アクセスは、記録、監視され、そうした情報は保持されることになります。AWS は論理的および物理的なモニタリングシステムから取得した情報を、必要に応じてセキュリティを向上させるために相関性を確認します。 AWS ではグローバルセキュリティオペレーションセンターを使用してデータセンターを監視しています。このグローバル・セキュリティ・オペレーションセンターは、モニタリング、対処優先順位の決定、および決定された処理を実施について責任をもっています。データセンターのアクセスを管理、モニタリングし、ローカルのチームと関連サポートチームと協力し、対処優先順位の決定、コンサルティング、分析、送信を行い、24 時間 365 日グローバルレベルのサポートを提供しています。	-	アマゾン ウェブ サービス: リスクとコンプライアンス AWS Webサイト : AWS のコントロール https://aws.amazon.com/jp/compliance/data-center/controls/

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実60	○	-	・火災検出と鎮火 自動火災検出および鎮火装置が取り付けられ、リスクを軽減しています。この火災検出システムは、全データセンター環境、機械的及び電気的インフラストラクチャースペース、冷却室および発電機設備室において、煙検出センサーを使用しています。これらのエリアは、充水型、二重連結予作動式、またはガス式スプリンクラーシステムによって守られています。 ・電力 データセンターの電力システムは、完全に冗長性をもち、運用に影響を与えることなく管理が可能となっています。 1 日24 時間体制で、年中無休で稼動しています。施設内で重要かつ不可欠な負荷に対応するために、電力障害時には無停電電源装置（UPS）がバックアップ電力を供給しています。データセンターは、発電機を使用して施設全体のバックアップ電力を供給しています。 ・空調と温度 サーバーその他のハードウェアの運用温度を一定に保つために、空調制御が必要です。これによって過熱を防ぎ、サーバー停止の可能性を減らすことができます。データセンターは、大気の状態を最適なレベルに保つように設定されています。作業員とシステムが、温度と湿度を適切なレベルになるよう監視してコントロールしています。 ・管理 AWS は、問題が速やかに特定されるように、電気、機械、ライフサポートシステムおよび設備を監視しています。予防的メンテナンスが実行され、設備の継続的な運用性が保たれています。	-	アマゾン ウェブ サービス：セキュリティプロセスの概要
実61	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実62	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実63	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実64	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実65	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実66	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実67	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実68	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実69	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実70	○	○	AWS は、様々な手段の外部コミュニケーションを実施して、その顧客ベースとコミュニティをサポートしてきました。カスタマーエクスペリエンスに影響を与える運用上の問題についてカスタマーサポートチームが通知受けることができるようにするためのメカニズムが配備されています。[Service Health Dashboard] が、顧客サポートチームによって管理運営されており、大きな影響を与える可能性のある問題について顧客に警告を発することができます。 カスタマーサポートチームと直接連絡を取ったり、お客様に影響を与える各種の問題に対する警告を事前に受け取ることができる AWS サポートに申し込みをすることもできます。 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。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 AWS サポートは、経験豊富な技術サポートエンジニアによる、1 対 1 の迅速なレスポンスを特徴とするサポートサービスです。AWS サポートは、お客様がそのインフラストラクチャをクラウドで運用できるように技術的な問題に関する支援を行います。操作上の問題や技術的な質問があるお客様は、サポートエンジニアのチームに連絡でき、予測可能な応答時間およびパーソナライズされたサポートを受けることができます。 AWSサポートの詳細については以下のURLをご参照ください。（https://aws.amazon.com/jp/premiumsupport/ ）	アマゾン ウェブ サービス：セキュリティプロセスの概要
実71	○	○	事業継続マネジメントに関する管理策はISO/IEC 27001に準拠しており、AWSのデータセンターにおける運用管理策についてはISO/IEC 27001認証を取得しています。ISO/IEC 27001の内容については ISO/IEC 27001 の附属書 A.17 をご参照ください。 Amazon のインフラストラクチャは高いレベルの可用性を備え、回復機能を持つ IT アーキテクチャを配備する機能を顧客に提供します。AWS のシステムは、お客様への影響を最小限に抑えながらシステムまたはハードウェア障害に耐えられるように設計されています。また、AWS におけるデータセンターの事業の継続性は、Amazon Infrastructure Group の指示に従って管理されます。 世界各地に設置されているデータセンターは、所在地によりリージョンに分けられています。すべてのデータセンターは オンラインでお客様にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動されます。重要なアプリケーションは N+1 原則でデプロイさ れます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。 AWS を使用すると、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、複数の地理上のリージョン内に、柔軟にインスタンスを配置してデータを保管できます。各アベイラビリティーゾーンは、障害が発生しても他のゾーンに影響を与えないように設計されています。つまり、アベイラビリティゾーンは、代表的な都市のリージョン内で物理的に区切られており、低リスクの氾濫原にあります(具体的な洪水帯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。アベイラビリティゾーンはすべて、複数の Tier-1 トランジットプロバイダに重複して接続しています。 AWS のバックアップおよび冗長性メカニズムは、ISO/IEC 27001 に準拠して開発され、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/IEC 27001 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。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 AWS サポートは、経験豊富な技術サポートエンジニアによる、1 対 1 の迅速なレスポンスを特徴とするサポートサービスです。AWS サポートは、お客様がそのインフラストラクチャをクラウドで運用できるように技術的な問題に関する支援を行います。操作上の問題や技術的な質問があるお客様は、サポートエンジニアのチームに連絡でき、予測可能な応答時間およびパーソナライズされたサポートを受けることができます。 AWSサポートの詳細については以下のURLをご参照ください。（https://aws.amazon.com/jp/premiumsupport/ ）	アマゾン ウェブ サービス：セキュリティプロセスの概要 アマゾン ウェブ サービス：リスクとコンプライアンス

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実72	○	○	AWS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。 インシデントや問題の処理時には、運用担当者を支援して情報を提供するための文書が保持されます。問題の解決のために協力体制が必要な場合は、情報伝達と記録機能をサポートする会議システムが使用されます。協力体制を必要とする運用上の問題の処理にあたっては、訓練を受けた通話リーダーが、コミュニケーションと進捗を支援します。 深刻な運用上の問題が発生した後には、外部的な影響の有無に関わらず、事後分析会議が開かれます。そしてエラーの原因（COE）に関する文書が起草され、根本的な原因が捕捉されて、今後のために予防措置が取られるようにします。予防措置の実施は、週に一度開かれる運用会議において追跡されます。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 AWS サポートは、経験豊富な技術サポートエンジニアによる、1 対 1 の迅速なレスポンスを特徴とするサポートサービスです。AWS サポートは、お客様がそのインフラストラクチャをクラウドで運用できるように技術的な問題に関する支援を行います。操作上の問題や技術的な質問があるお客様は、サポートエンジニアのチームに連絡でき、予測可能な応答時間およびパーソナライズされたサポートを受けることができます。 AWSサポートの詳細については以下のURLをご参照ください。（https://aws.amazon.com/jp/premiumsupport/ ）	アマゾン ウェブ サービス：セキュリティプロセスの概要

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実73	○	○	[BCP(Business Continuity Plan)；事業継続計画] AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。 [パンデミックへの対応] AWS は、感染症の爆発的な流行の脅威に対して迅速に対応するための準備として、パンデミック対応ポリシーと手順を災害復旧計画に組み込んでいます。関連したリスクに関する軽減のためのストラテジーには、重要なプロセスをリージョン外のリソースに移動するために、どのようにスタッフを配置するかという代替モデルと、重要なビジネス業務をサポートするための危機管理の発動計画が含まれます。パンデミック計画は、国際的な健康関連機関や規制に従っていますが、国際的な関連機関との連絡窓口等も含まれています。 [事業継続性管理] Amazon のインフラストラクチャは高いレベルの可用性を備え、回復機能を持つ IT アーキテクチャを配備する機能を顧客に提供します。AWS のシステムは、お客様への影響を最小限に抑えながらシステムまたはハードウェア障害に耐えられるように設計されています。また、AWS におけるデータセンターの事業の継続性は、Amazon Infrastructure Group の指示に従って管理されます。 [可用性] 世界各地に設置されているデータセンターは、所在地によりリージョンに分けられています。すべてのデータセンターはオンラインでお客様にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。 AWS を使用すると、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、複数の地理上のリージョン内に、柔軟にインスタンスを配置してデータを保管できます。 各アベイラビリティーゾーンは、障害が発生しても他のゾーンに影響を与えないように設計されています。つまり、アベイラビリティゾーンは、代表的な都市のリージョン内で物理的に区切られており、低リスクの氾濫原にあります（具体的な洪水帯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。アベイラビリティゾーンはすべて、複数の Tier-1 トランジットプロバイダに重複して接続しています。AWS の使用量は、複数のリージョンやアベイラビリティーゾーンを利用できるように設計することをお勧めします。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置すると、自然災害やシステム障害を含むほとんどの障害が発生したときに、回復力を持った状態を保つことができます。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	AWS Webサイト：AWS のコントロール - 物理アクセスビジネスの継続性と災害復旧 https://aws.amazon.com/jp/compliance/data-center/controls/ アマゾン ウェブ サービス：セキュリティプロセスの概要

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
			[インシデントへの対応] 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。 [役員による全社的検査] Amazon の内部監査グループは、最近になって AWS サービスの復元プランを検査しました。このプランは、上級役員管理チームと取締役の監査委員会のメンバーによっても定期的に検査されています。 [コミュニケーション] 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。これらの方法には、新入社員向けのオリエンテーションとトレーニングプログラム、業績その他についてアップデートを行う定例のマネジメント会議、ビデオ会議、電子メールメッセージ、Amazon イントラネットでの情報の投稿などの電子的手段があります。		
実74	○	○	・世界各地に設置されているデータセンターは、所在地によりリージョンに分けられています。すべてのデータセンターはオンラインでお客様にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。 AWS を使用すると、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、複数の地理上のリージョン内に、柔軟にインスタンスを配置してデータを保管できます。各アベイラビリティーゾーンは、障害が発生しても他のゾーンに影響を与えないように設計されています。つまり、アベイラビリティゾーンは、代表的な都市のリージョン内で物理的に区切られており、低リスクの氾濫原にあります（具体的な洪水帯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。アベイラビリティゾーンはすべて、複数の Tier-1 トランジットプロバイダに重複して接続しています。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	アマゾン ウェブ サービス： セキュリティプロセスの概要
実75	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実76	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実77	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実78	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実79	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実80	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

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。

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実81	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実82	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実83	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実84	○	○	・Amazon のインフラストラクチャは高いレベルの可用性を備え、回復機能を持つ IT アーキテクチャを配備する機能を顧客に提供します。AWS のシステムは、お客様への影響を最小限に抑えながらシステムまたはハードウェア障害に耐えられるように設計されています。また、AWS におけるデータセンターの事業の継続性は、Amazon Infrastructure Group の指示に従って管理されます。 ・世界各地に設置されているデータセンターは、所在地によりリージョンに分けられています。すべてのデータセンターはオンラインでお客様にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 クラウド環境においてはハードウェアの冗長化のみならず、ソフトウェアによるサービスの冗長化構成も高可用性を実現するために重要な要素となります。 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/アベイラビリティーゾーンのデプロイアーキテクチャなどです。 また、お客様はAmazon EC2 Auto Scalingを使用することができます。Amazon EC2 Auto Scaling は、Amazon EC2 のインスタンスを自動的に作成または終了してアプリケーションの負荷を処理する Amazon EC2 インスタンスの数を調整できる、完全マネージド型サービスです。Amazon EC2 Auto Scaling では、異常なインスタンスを検出して置き換えることにより、EC2 インスタンスのフリートを管理できます。また、お客様が定義する条件に応じて Amazon EC2 のキャパシティーのスケールアップ/スケールダウンを自動的に行って、アプリケーションの可用性を維持できます。	アマゾン ウェブ サービス：セキュリティプロセスの概要
実85	○	○	・Amazon のインフラストラクチャは高いレベルの可用性を備え、回復機能を持つ IT アーキテクチャを配備する機能を顧客に提供します。AWS のシステムは、お客様への影響を最小限に抑えながらシステムまたはハードウェア障害に耐えられるように設計されています。また、AWS におけるデータセンターの事業の継続性は、Amazon Infrastructure Group の指示に従って管理されます。 ・世界各地に設置されているデータセンターは、所在地によりリージョンに分けられています。すべてのデータセンターはオンラインでお客様にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 クラウド環境においてはハードウェアの冗長化のみならず、ソフトウェアによるサービスの冗長化構成も高可用性を実現するために重要な要素となります。 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/アベイラビリティーゾーンのデプロイアーキテクチャなどです。	アマゾン ウェブ サービス：セキュリティプロセスの概要

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実86	○	○	・Amazon のインフラストラクチャは高いレベルの可用性を備え、回復機能を持つ IT アーキテクチャを配備する機能を顧客に提供します。AWS のシステムは、お客様への影響を最小限に抑えながらシステムまたはハードウェア障害に耐えられるように設計されています。また、AWS におけるデータセンターの事業の継続性は、Amazon Infrastructure Group の指示に従って管理されます。 ・世界各地に設置されているデータセンターは、所在地によりリージョンに分けられています。すべてのデータセンターはオンラインでお客様にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 クラウド環境においてはハードウェアの冗長化のみならず、ソフトウェアによるサービスの冗長化構成も高可用性を実現するために重要な要素となります。 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/アベイラビリティーゾーンのデプロイアーキテクチャなどです。	アマゾン ウェブ サービス：セキュリティプロセスの概要
実87	○	○	各データセンター間は物理的に離れており、冗長性のある電源とネットワーキングを備えています。 AWS ネットワークのインターネット側のそれぞれの境界では、複数の通信サービスへの重複する接続を採用しています。これらの接続にはそれぞれ、専用ネットワークデバイスがあります。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 クラウド環境においてはハードウェアの冗長化のみならず、ソフトウェアによるサービスの冗長化構成も高可用性を実現するために重要な要素となります。 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/アベイラビリティーゾーンのデプロイアーキテクチャなどです。	AWS Webサイト：データセンター - 環境レイヤー https://aws.amazon.com/jp/compliance/data-center/environmental-layer/ アマゾン ウェブ サービス：セキュリティプロセスの概要
実88	○	○	（実87と同様）	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 クラウド環境においてはハードウェアの冗長化のみならず、ソフトウェアによるサービスの冗長化構成も高可用性を実現するために重要な要素となります。 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/アベイラビリティーゾーンのデプロイアーキテクチャなどです。	アマゾン ウェブ サービス：セキュリティプロセスの概要
実89	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実90	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実91	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実92	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実93	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実94	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実95	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実96	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実97	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実98	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実99	○	○	・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/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 ・Amazon の法人アプリケーションチームは、ソフトウェアの開発と管理を行って、サードパーティのソフトウェア配布、内部開発ソフトウェアと設定管理の領域で、UNIX/Linux ホストの IT プロセスを自動化します。インフラストラクチャチームは、UNIX/Linux 設定管理フレームワークを運用して、ハードウェアの拡張性、可用性、監査、セキュリティ管理を解決します。変更管理の自動プロセスを使用した集中管理ホストにより、当社は、高可用性、再現性、拡張性、セキュリティおよび障害復旧という目標を達成することが可能となります。システムおよびネットワークエンジニアは、これらの自動ツールのステータスを日常的にモニタリングしており、レポートを検証して、設定やソフトウェアの取得または更新に失敗するホストへの対応を行っています。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 AWS Systems Manager を使用することで、複数の AWS のサービスの運用データを一元化し、AWS リソース全体のタスクを自動化できます。アプリケーション、アプリケーションスタックのさまざまなレイヤー、本番環境と開発環境といったリソースの論理グループを作成できます。Systems Manager では、リソースグループを選択し、その最新の API アクティビティ、リソース設定の変更、関連する通知、運用アラート、ソフトウェアインベントリ、パッチコンプライアンス状況を表示できます。運用ニーズに応じて、各リソースグループに対してアクションを実行することもできます。Systems Manager により、AWS リソースを一元的に表示および管理でき、運用を完全に可視化して制御できます。 ・AWS CloudFormation は、開発や本運用に必要な、互いに関連する AWS およびサードパーティのリソースコレクションを作成し、そのリソースを適切な順序でプロビジョニングするためのサービスです。AWS CloudFormation を使用すれば、アプリケーションを駆動する関連リソースのグループを予測可能な方法で繰り返し作成する作業を自動化および簡素化できます。	アマゾン ウェブ サービス：AWS リスクとコンプライアンス アマゾン ウェブ サービス：セキュリティプロセスの概要 AWS Webサイト：AWS Systems Managerのよくある質問 https://aws.amazon.com/jp/systems-manager/faq/ AWS Webサイト：AWS CloudFormation のよくある質問 https://aws.amazon.com/jp/cloudformation/faqs/
実100	○	○	・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/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 ・AWSにおける変更は、通常、影響が最も少ない領域から段階的な展開で運用環境にプッシュされます。 導入は単一のシステムでテストされ、影響を評価できるよう、綿密に監視されます。 サービス所有者は、サービスのアップストリーム依存関係の健全性を測定する設定可能なメトリックを多数持っています。 これらのメトリックスは、しきい値とアラームが所定の位置に密接に監視されます。 ロールバック手順は、変更管理 (CM) チケットに記載されています。 可能な場合、変更は通常の変更ウィンドウ中にスケジュールされます。 標準の変更管理手順からの逸脱を必要とする本番システムへの緊急の変更は、インシデントに関連付けられ、必要に応じてログに記録され、承認されます。 AWS は、重要なサービスの変更に対する自己監査を定期的に行っており、品質をモニタリングしながら高い基準を維持することによって、変更管理プロセスの継続的な改善に貢献しています。例外は分析され、根本的な原因が決定されて適切な措置が取られます。変更はコンプライアンスに従うようにされるか、または必要に応じてロールバックされます。その後プロセスまたは人的問題を解決して修正するための措置が取られます。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	アマゾン ウェブ サービス：AWS リスクとコンプライアンス アマゾン ウェブ サービス：セキュリティプロセスの概要

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。

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実101	○	○	AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティーに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティープランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 Amazon CloudWatch は、AWS クラウドリソースと AWS で実行されるアプリケーションのモニタリングサービスです。お客様は、Amazon CloudWatch を使用して、メトリクスを収集/追跡し、ログファイルを収集してモニタリングし、アラームを設定できます。Amazon CloudWatch は、Amazon EC2 インスタンス、Amazon DynamoDB テーブル、Amazon RDS DB インスタンスなどの AWS リソース、アプリケーションやサービスに生成されたカスタムメトリクス、アプリケーションが生成するあらゆるログファイルをモニタリングできます。Amazon CloudWatch を使用して、リソース使用率、アプリケーションパフォーマンス、オペレーションの状態においてシステム全体の可視性を得られます。	AWS Webサイト：AWS のコントロール – キャパシティの管理 https://aws.amazon.com/jp/compliance/data-center/controls/
実102	○	○	AWS は、様々な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。 AWS モニタリングツールは、異常な、または不正なアクティビティと条件を通信の出入り口で検出するように設計されています。これらのツールは、サーバーおよびネットワークの利用状況、ポートスキャニングアクティビティ、アプリケーションの利用状況、および許可されていない侵入の試みをモニタリングします。このツールを使用して、異常なアクティビティに対して独自に性能測定基準のしきい値を設定することができます。 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。主要なオペレーションメトリックが早期警告しきい値を超えた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（常時待機体制）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することができます。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 Amazon CloudWatch は、AWS クラウドリソースと AWS で実行されるアプリケーションのモニタリングサービスです。お客様は、Amazon CloudWatch を使用して、メトリクスを収集/追跡し、ログファイルを収集してモニタリングし、アラームを設定できます。Amazon CloudWatch は、Amazon EC2 インスタンス、Amazon DynamoDB テーブル、Amazon RDS DB インスタンスなどの AWS リソース、アプリケーションやサービスに生成されたカスタムメトリクス、アプリケーションが生成するあらゆるログファイルをモニタリングできます。Amazon CloudWatch を使用して、リソース使用率、アプリケーションパフォーマンス、オペレーションの状態においてシステム全体の可視性を得られます。	アマゾン ウェブ サービス：セキュリティプロセスの概要
実103	○	○	AWS は、様々な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。 AWS モニタリングツールは、異常な、または不正なアクティビティと条件を通信の出入り口で検出するように設計されています。これらのツールは、サーバーおよびネットワークの利用状況、ポートスキャニングアクティビティ、アプリケーションの利用状況、および許可されていない侵入の試みをモニタリングします。このツールを使用して、異常なアクティビティに対して独自に性能測定基準のしきい値を設定することができます。 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。主要なオペレーションメトリックが早期警告しきい値を超えた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（常時待機体制）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することができます。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 Amazon CloudWatch は、AWS クラウドリソースと AWS で実行されるアプリケーションのモニタリングサービスです。お客様は、Amazon CloudWatch を使用して、メトリクスを収集/追跡し、ログファイルを収集してモニタリングし、アラームを設定できます。Amazon CloudWatch は、Amazon EC2 インスタンス、Amazon DynamoDB テーブル、Amazon RDS DB インスタンスなどの AWS リソース、アプリケーションやサービスに生成されたカスタムメトリクス、アプリケーションが生成するあらゆるログファイルをモニタリングできます。Amazon CloudWatch を使用して、リソース使用率、アプリケーションパフォーマンス、オペレーションの状態においてシステム全体の可視性を得られます。	アマゾン ウェブ サービス：セキュリティプロセスの概要

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実104	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実105	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実106	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実107	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実108	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実109	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実110	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実111	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実112	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実113	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実114	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実115	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実116	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実117	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実118	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実119	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実120	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実121	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実122	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実123	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実124	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実125	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実126	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実127	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実128	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実129	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実130	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実131	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実132	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実133	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実134	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実135	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実136	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実137	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実138	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実139	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

「対応の主体」凡例　○ ：主体として対応する
- ：必要に応じて情報を提供する

基準番号	対応の主体		AWSの対応状況	お客様が統制すべき内容	補足情報
	AWS	お客様			
実140	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実141	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実142	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実143	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実144	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実145	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実146	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実147	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実148	-	○	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

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。

「対応の主体」凡例　○：主体として対応する
　　-　：必要に応じて情報を提供する

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
監1	1	-	○	・以下の情報を参考にAWSを外部委託先としての監査にお役立てください。 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 にデプロイされている部分では、AWS が該当する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、統制することになります。AWS で定めている統制の内容と、その統制がどのように効果的に運用されているかについて、AWS では SOC1 Type II レポートを発行し、EC2、S3、VPC などに関連し定義された統制、ならびに詳細な物理セキュリティおよび環境に関する統制を公表しています。これらの統制は、ほとんどのお客様のニーズに見合うように、ハイレベルで定義されています。AWS と機密保持契約を結んでいる AWS のお客様は、SOC1 Type II レポートを要求できます。	-
	2	-	○	-	-
	3	-	○	・以下の情報を参考にAWSを外部委託先としての監査にお役立てください。 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。	-
	4	-	○	・以下の情報を参考にAWSを外部委託先としての監査にお役立てください。 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、お客様の責任範囲となります。AWS 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。このレポートはお客様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/IEC 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。 事実確認および意見交換等に関するお問い合わせは担当営業までご連絡ください。	-
	5	-	○	・以下の情報を参考にAWSを外部委託先としての監査にお役立てください。 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/IEC 27001 監査、PCI 評価、ITAR 監査、FedRAMP テストプログラムの一部となっています。	-

変更履歴

■ 2020年9月 第9版令和2年3月版の反映
■ 2022年5月 第9版令和3年12月版の反映、一部情報の更新

基準番号	枝番	AWSの対応状況(旧)	AWSの対応状況(新)
統20	3-(12)	・AWS では 160 種類を超えるクラウドサービスについて従量制料金を適用しています。 AWS では必要な個々のサービスにのみ、サービスを使用する期間だけお支払いいただき、長期契約や複雑なライセンスは必要ありません。 サービスを消費した分だけ支払い、サービスの使用を停止したときの追加コストや解約料金はありません。 https://aws.amazon.com/jp/pricing/	AWS では 200 種類を超えるクラウドサービスについて従量制料金を適用しています。 https://aws.amazon.com/jp/pricing/
統20 統21 統24	3-(14) 1, 2 1, 2	~~・2017年11月より日本のお客様に向けて「日本準拠法に関する AWS カスタマーアグリーメント変更契約」の手続きが可能な新機能の提供を開始しました。これにより、AWS Artifact を通じて日本準拠法に関する AWS カスタマーアグリーメント変更契約をリアルタイムに締結または終了することが可能となっています。日本準拠法に関する AWS カスタマーアグリーメント変更契約とは、現在お客様がご利用中の AWS アカウントに適用されている、AWS カスタマーアグリーメントの準拠法および管轄裁判所を変更する契約を指します。この契約を有効にすることで、AWS カスタマーアグリーメントの準拠法を日本法に変更し、更に、同契約に関するあらゆる紛争に関する第一審裁判所を東京地方裁判所に変更することができます。~~ ~~従来、AWSカスタマーアグリーメントの準拠法および管轄裁判所を変更する際に、その都度、書面で契約を締結して頂く必要がありましたが、AWSアカウントのマネジメントコンソールからお客様ご自身で受諾（有効に）することで、お客様の手間を省略することが可能となっています。~~ ~~https://aws.amazon.com/jp/blogs/news/how-to-change-aws-ca-by-~~	・AWSのカスタマーアグリーメントにおいて、クラウドサービスの販売者がアマゾン ウェブ サービス ジャパン合同会社のアカウントについては「準拠法」を日本国法、「管轄裁判所」を東京地裁と定めています。
統27 (新設)	–	–	–
実20	–	–	実21と整合させるため追加。また、対応の主体のAWSにも〇を追加。 --- 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/IEC 27001 に準拠しています。 詳細についてはISO/IEC 27001 の附属書 A、ドメイン 12 を参照してください。AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 また、Amazon の資産 (ノートパソコンなど) は、E メールのフィルタリングとマルウェア検出を含むウイルス対策ソフトウェアで設定されています。 AWS ネットワークファイアウォール管理および Amazon のウイルス対策プログラムは、SOC、PCI DSS、ISO/IEC 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。
実145 (新設)	–	–	–
実146 (新設)	–	–	–
実147 (新設)	–	–	–
実148 (新設)	–	–	–