「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	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1	5	-	○	-	すべての AWS API と CLI リクエストに対して、長期的認証情報ではなく一時的なセキュリティ認証情報を使用します。AWS サービスに対する API および CLI リクエストは、ほとんどの場合、AWS アクセスキーを使って署名する必要があります。これらのリクエストの署名に使用する認証情報は、一時的でも長期的でもかまいません。長期的認証情報 (長期的アクセスキー) を使用すべき唯一の状況は、IAM ユーザーまたは AWS アカウント ルートユーザーを使用している場合です。AWS に対してフェデレーションを行うか、または他の方法により IAM ロールを担う場合、一時的認証情報が生成されます。サインイン認証情報を使って AWS Management Console にアクセスしても、AWS サービスへのコールを行うために一時的な認証情報が生成されます。長期的認証情報が必要な状況はほとんどなく、一時的な認証情報でほとんどのタスクを遂行できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_identities_unique.html ユーザーが各自のパスワードを変更できるように許可する場合は、強力なパスワードを作成することをユーザーに要求するパスワードポリシーを作成します。 IAM ユーザーのデフォルトのパスワードポリシーでは、次の条件が適用されます。 ・パスワードの文字数制限: 8 ～ 128 文字 ・大文字、小文字、数字、! @ # $ % ^ & * ( ) _ + - = [ ] { } | ' 記号のうち、最低 3 つの文字タイプの組み合わせ ・AWS アカウント名または E メールアドレスと同じでないこと 必要に応じて、IAM コンソールの [Account Settings] (アカウント設定) ページで、AWS アカウントのカスタムパスワードポリシーを作成できます。AWS のデフォルトのパスワードポリシーからアップグレードして、最小文字数、アルファベット以外の文字が必要かどうか、変更頻度など、パスワードの要件を定義します。詳細については、「IAM ユーザー用のアカウントパスワードポリシーの設定」を参照してください。 ID の使用者のみがパスワードを知っている状態を担保するため、ID を発行後、初回サインイン時にパスワードの変更を強制します。IAM ユーザーに初回サインイン時に新しいパスワードの作成を求めるには、AWS マネジメントコンソールの IAM ユーザー作成ウィザードで、[Require password reset (パスワードのリセットが必要)] を選択します。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md	AWS Well-Architected フレームワーク セキュリティの柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html AWS Well-Architected フレームワーク FSI Lens for FISC セキュリティの柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md
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。	-

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実3	8	-	○	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。 加えて、詳細についてはAWSクラウドセキュリティホワイトペーパー (http://aws.amazon.com/security で入手可能) を参照してください。 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 認定をセキュリティ保護、配布するために使用されます。 AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。	キーの保存、ローテーション、アクセス制御を含む暗号化アプローチを定義することで、不正ユーザーからのコンテンツの保護や、正規ユーザーへの不必要な公開を防止することができます。AWS Key Management Service (AWS KMS) は暗号化キーの管理をサポートして 多数の AWS のサービスと統合します.このサービスでは、AWS KMS キーのための、耐久性と安全性が高く、冗長なストレージを利用できます。キーのエイリアスのほか、キーレベルのポリシーも定義できます。ポリシーは、キー管理者やキーユーザーを定義するのに役立ちます。さらに、AWS CloudHSM はクラウドベースのハードウェアセキュリティモジュール (HSM) であり、AWS クラウド 上で独自の暗号化キーを簡単に生成して使用できます。FIPS 140-2 レベル 3 検証済みの HSM を使用することで、データセキュリティに関する企業、契約、規制のコンプライアンス要件を満たすことができます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_data_rest_key_mgmt.html	AWS Well-Architected フレームワーク セキュリティの柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html アマゾン ウェブ サービス：リスクとコンプライアンス https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf
実3	参考3	-	○	-	AWS Key Management Service (AWS KMS) は、アプリケーションと AWS のサービス全体で暗号キーを作成、管理、制御することができます。 AWS KMS は、暗号化と復号化のための KMS キーを作成する際に 256 ビットのキーをサポートします。発信者に返される生成済みデータキーは、256 ビット、128 ビット、または最大 1024 バイトまでの任意の値にすることができます。AWS KMS でお客様の代わりに 256 ビットの KMS キーを使用して暗号化または復号化を行う場合、Galois Counter Mode の AES アルゴリズム (AES-GCM) が使用されます。カスタマー管理の KMS キーのライフサイクルを管理し、誰がそれを使用または管理できるかを管理します。AWS KMS がキーを自動的にローテーションすることを選択した場合は、データを再暗号化する必要はありません。AWS KMS は過去のバージョンのキーを自動的に保管して、そのキーで暗号化されたデータを復号化できるようにします。AWS KMS のキーに対する新しい暗号化リクエストは、すべて最新バージョンのキーで実行されます。 https://docs.aws.amazon.com/ja_jp/kms/latest/cryptographic-details/crypto-primitives.html"	AWS KMS の暗号化の詳細説明 https://docs.aws.amazon.com/ja_jp/kms/latest/cryptographic-details/intro.html AWS Well-Architected フレームワーク FSI Lens for FISC セキュリティの柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md
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4	5	-	○	-	暗号化キーと証明書を安全に保存し、厳格なアクセスコントロールによって適切な時間間隔でローテーションします。これを実現する最善の方法として、 AWS Certificate Manager (ACM).これにより、AWS のサービスおよび内部接続リソースで使用するためのパブリックおよびプライベートの Transport Layer Security (TLS) 証明書のプロビジョニング、管理、デプロイが容易になります。TLS 証明書は、ネットワーク通信を保護し、プライベートネットワーク上のリソースだけでなく、インターネット上のウェブサイトのアイデンティティを確立するために使用されます。ACM は、Elastic Load Balancers (ELB)、AWS ディストリビューション、API Gateway の API などの AWS リソース と統合し、証明書の自動更新も処理します。Amazon Elastic Compute Cloud を使用してプライベートルート CA をデプロイする場合、証明書とプライベートキーの両方を ACM (Amazon EC2) インスタンス、コンテナなどで使用するために提供できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_data_transit_key_cert_mgmt.html	AWS Well-Architected フレームワーク セキュリティの柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
					AWS のサービスには、通信に TLS を使用し、AWS API との通信の際に伝送中データの暗号化を利用できる、HTTPS エンドポイントが用意されています。HTTP など安全でないプロトコルは、セキュリティグループを使用して VPC で監査およびブロックできます。HTTP リクエストは、Amazon CloudFront または Application Load Balancer でHTTPS に自動的にリダイレクトすることもできます。コンピューティングリソースを完全に制御して、サービス全体に伝送中データの暗号化を実装できます。また、外部ネットワークまたは AWS Direct Connect からお使いの VPC に VPN で接続して、トラフィックの暗号化を促進できます。クライアントが AWS API に電話かける際に、最低でも TLS 1.2 を使用していることを確認してください。AWS は、2023 年 6 月に TLS 1.0 と 1.1 の使用を廃止予定です。特別な要件がある場合は、AWS Marketplace でサードパーティーのソリューションを入手できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_data_transit_encrypt.html	
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5	3	-	○	-	アクセス (最小特権を使用)、分離、バージョニングなど、複数のコントロールによって保管中のデータを保護できます。データへのアクセスは、AWS CloudTrail などの探査メカニズムと、Amazon Simple Storage Service (Amazon S3) アクセスログなどのサービスレベルログを使用して監査する必要があります。パブリックにアクセス可能なデータをインベントリし、時間の経過とともにパブリックで利用可能なデータ量の削減します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_data_rest_access_control.html lAWS リソースへのアクセス権限について、付与されている権限のうち、利用されていない権限について AWS Identity and Access Management (IAM) アクセスアドバイザーで最終アクセス時間を確認することで検出することが可能になります。アクセス権限の妥当性について確認を行い、不要であれば削除します。インバウンドトラフィックとアウトバウンドトラフィックの両方について、多層防御アプローチでコントロールを適用します。たとえば、Amazon Virtual Private Cloud (VPC) の場合、これにはセキュリティグループ、ネットワーク ACL、サブネットが含まれます。重要なファイルへのアクセスについて、VPC からのみアクセスを許可することで、ネットワークレイヤでの対策を追加することが可能になります。例えば Amazon S3 に保存する場合、VPC エンドポイントやパブリックブロックアクセスを活用することで実現することが可能です。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md	AWS Well-Architected フレームワーク セキュリティの柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html AWS Well-Architected フレームワーク FSI Lens for FISC セキュリティの柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md
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。	-

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実7	2	-	○	-	暗号化キーと証明書を安全に保存し、厳格なアクセスコントロールによって適切な時間間隔でローテーションします。これを実現する最善の方法として、 AWS Certificate Manager (ACM).これにより、AWS のサービスおよび内部接続リソースで使用するためのパブリックおよびプライベートの Transport Layer Security (TLS) 証明書のプロビジョニング、管理、デプロイが容易になります。TLS 証明書は、ネットワーク通信を保護し、プライベートネットワーク上のリソースだけでなく、インターネット上のウェブサイトのアイデンティティを確立するために使用されます。ACM は、Elastic Load Balancers (ELB)、AWS ディストリビューション、API Gateway の API などの AWS リソース と統合し、証明書の自動更新も処理します。Amazon Elastic Compute Cloud を使用してプライベートルート CA をデプロイする場合、証明書とプライベートキーの両方を ACM (Amazon EC2) インスタンス、コンテナなどで使用するために提供できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_data_transit_key_cert_mgmt.htm IAWS のサービスには、通信に TLS を使用し、AWS API との通信の際に伝送中データの暗号化を利用できる、HTTPS エンドポイントが用意されています。HTTP など安全でないプロトコルは、セキュリティグループを使用して VPC で監査およびブロックできます。HTTP リクエストは、Amazon CloudFront または Application Load Balancer でHTTPS に自動的にリダイレクトすることもできます。コンピューティングリソースを完全に制御して、サービス全体に伝送中データの暗号化を実装できます。また、外部ネットワークまたは AWS Direct Connect からお使いの VPC に VPN で接続して、トラフィックの暗号化を促進できます。クライアントが AWS API に電話かける際に、最低でも TLS 1.2 を使用していることを確認してください。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_data_transit_encrypt.html	AWS Well-Architected フレームワーク セキュリティの柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html
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8	7	-	○	-	人的 ID が AWS にサインインする方法は多数あります。AWS ベストプラクティスは、AWS に認証する際にフェデレーション (直接フェデレーションまたは AWS IAM Identity Center (successor to AWS Single Sign-On) を使用) を使って、一元化された ID プロバイダーに依存する方法です。 この場合、ID プロバイダーまたは Microsoft Active Directory を使って、セキュアなサインインプロセスを確立する必要があります。最初に AWS アカウント を開いたとき、AWS アカウント ルートユーザーから始めます。 ユーザー (およびルートユーザーを必要とする タスク) へのアクセスを設定するには、アカウントのルートユーザーのみを使用する必要があります。.AWS アカウント を開いた直後にアカウントのルートユーザーに対して MFA を有効化し、AWS ベストプラクティスガイドを使用してルートユーザーをセキュリティ保護することが重要です。AWS IAM Identity Center (successor to AWS Single Sign-On) でユーザーを作成する場合、そのサービスでサインインプロセスをセキュリティ保護します。 消費者アイデンティティについては、Amazon Cognito user pools を使用して、そのサービスで、またはAmazon Cognito user pools がサポートする ID プロバイダーの 1 つを使ってサインインプロセスをセキュリティ保護します。AWS Identity and Access Management (IAM) ユーザーを使用している場合、IAM を使ってサインインプロセスをセキュリティ保護することになります。サインイン方法に関係なく、強力なサインインポリシーを適用することが不可欠です。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_identities_enforce_mechanisms.html	AWS Well-Architected フレームワーク セキュリティの柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実8	参考4	-	○	-	すべての AWS API と CLI リクエストに対して、長期的認証情報ではなく一時的なセキュリティ認証情報を使用します。AWS サービスに対する API および CLI リクエストは、ほとんどの場合、AWS アクセスキーを使って署名する必要があります。これらのリクエストの署名に使用する認証情報は、一時的でも長期的でもかまいません。長期的認証情報 (長期的アクセスキー) を使用すべき唯一の状況は、IAM ユーザーまたは AWS アカウント ルートユーザーを使用している場合です。AWS に対してフェデレーションを行うか、または他の方法により IAM ロールを担う場合、一時的認証情報が生成されます。サインイン認証情報を使って AWS Management Console にアクセスしても、AWS サービスへのコールを行うために一時的な認証情報が生成されます。長期的認証情報が必要な状況はほとんどなく、一時的な認証情報でほとんどのタスクを遂行できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_identities_unique.html	AWS Well-Architected フレームワーク セキュリティの柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html
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9	2	-	○	-	AWS アカウント を作成する場合は、このアカウントのすべての AWS のサービス とリソースに対して完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることによってアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報を保護し、それらを使用してルートユーザーのみが実行できるタスクを実行します。 https://docs.aws.amazon.com/ja_jp/accounts/latest/reference/root-user.html 以下は、アカウントのルートユーザーを保護するためのベストプラクティスです。 https://docs.aws.amazon.com/ja_jp/accounts/latest/reference/best-practices-root-user.html	
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10	8	-	○	-	マネジメントコンソールのアクセス履歴はCloudTrailに記録されます。 https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-event-reference-aws-console-sign-in-events.html CloudTrail が配信した後でログファイルが変更、削除、または変更されなかったかどうかを判断するには、CloudTrail ログファイルの整合性の検証を使用することができます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。AWS CLI を使用して CloudTrail が配信した場所のファイルを検証することができます。 https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html	

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実10	9	-	○	-	CloudTrailのイベントは協定世界時(UTC)で出力されます。 https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-event-reference-record-contents.html Amazon では、Amazon Time Sync Service を提供します。このサービスはすべての EC2 インスタンスからアクセスでき、その他の AWS のサービス にも利用されます。このサービスは、各 AWS リージョン で衛星接続された原子基準クロックを使用し、ネットワークタイムプロトコル (NTP) を通じて世界標準時 (UTC) の現在の正確な現在時刻を表示します。Amazon Time Sync Service は、UTC に追加されたうるう秒を自動的に均一化します。 https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/set-time.html すべての Amazon RDS DB インスタンスは、デフォルトで UTC/GMT 時間を使用します。タイムゾーンの変更は任意です。データベースレイヤーでは UTC タイムゾーンを使用するのがベストプラクティスです。UTC では夏時間 (DST) が適用されないため、夏時間の日付となっても時刻を調整する必要はありません。ローカルタイムゾーンを使用する必要がある場合は、代わりにアプリケーションレイヤーでタイムゾーンを変更してください。その際、事前にデータベース管理者またはアプリケーションチームに相談してください。 https://repost.aws/ja/knowledge-center/rds-change-time-zone CloudWatch ダッシュボードのタイムゾーン形式を変更して、ダッシュボードのデータを UTC またはローカルタイムで表示することもできます。ローカルタイムは、コンピュータのオペレーティングシステムで指定されているタイムゾーンです。 https://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/monitoring/change_dashboard_time_format.html	
実10	参考2	-	○	-	各アカウントで AWS CloudTrail をオンにして、サポートされている各リージョンで使用します。アクセスが非常に制限されている一元化されたログアカウントに AWS CloudTrail ログを保存します。CloudTrail ログファイルの整合性の検証を使用することでログファイル自体が変更されていないこと、または特定のユーザーの認証情報が特定の API アクティビティを実行したことを確実に検証することができます。 CloudTrail ログファイルの整合性の検証プロセスでは、ログファイルが削除または変更されたかどうかを知ることもできます。また、指定された期間内にログファイルがアカウントに配信されていないことを確実に検証することが可能です。CloudTrail ログファイルを定期的に調べます。 また、AWS CloudTrail イベント、VPC フローログ、DNS ログを継続的に分析することで脅威を検出するサービスである GuardDuty を使用することもできます。Amazon S3 バケットのロギングを有効にして、各バケットに対して行われたリクエストを監視します。アカウントが不正に使用されたと考えられる場合は、発行された一時的な認証情報に注意してください。 認識できない一時的な認証情報が発行された場合は、それらのアクセス許可を無効にします。サービスの最終アクセス時間データを使用して、IAM ロールを定期的に確認します。IAM エンティティ (ユーザーまたはロール) が最後にサービスにアクセスを試みたときのレポートを表示できます。次に、その情報を使用してポリシーを調整し、使用中のサービスのみへのアクセスを許可することができます。IAM のリソースの種類ごとにレポートを生成できます。詳細については、サービスの最終アクセス時間データの表示プロセスのドキュメントをお読みください。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md	AWS Well-Architected フレームワーク FSI Lens for FISC セキュリティの柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md
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	枝番	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13	4	-	○	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。 加えて、詳細についてはAWSクラウドセキュリティホワイトペーパー (http://aws.amazon.com/security で入手可能) を参照してください。 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 認定をセキュリティ保護、配布するために使用されます。 AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。	AWS Key Management Service (AWS KMS) は、カスタマーマスターキー (CMK) によるエンベロープ暗号化戦略を採用しています。エンベロープ暗号化は、平文データをデータキーで暗号化し、次にデータキーを別のキー、即ち CMK で暗号化する方法です。AWS KMS の外部でデータの暗号化に利用するデータキーは、CMK により生成、暗号化、復号されています。CMK は AWS KMS で作成され、暗号化されていない状態のままになることはありません。AWS KMS は、カスタマー管理の CMK、AWS 管理の CMK、AWS 所有の CMK という 3 種類の CMK をサポートします (詳細については、https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys を参照してください)。多くの金融機関のお客様にとって、カスタマー管理の CMK は、お客様のアプリケーションと AWS のサービスの両方からのアクセス権限を管理できるため推奨されます。カスタマー管理の CMK は、キーの生成や保管にさらなる柔軟性も提供します。また、キーの使用またはポリシーの変更はすべて、監査目的で AWS CloudTrail を用いて記録します。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md	AWS Well-Architected フレームワーク FSI Lens for FISC セキュリティの柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md アマゾン ウェブ サービス：リスクとコンプライアンス https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf
実13	5	-	○	-	データの暗号化を行う際は、暗号化を行う秘密鍵の管理者とデータを所有するリソースの管理者を分離することでより強固なセキュリティ対策を採用することが可能です。AWS KMS でカスタマーマネージドキーを使用することで、キーポリシーによりアクセス許可を定義することが可能になります。例えば、故意/過失に依らず Amazon S3 内のオブジェクトを不特定多数のインターネットに公開してしまった場合でも、暗号化を行う秘密鍵のキーポリシーでインターネットから秘密鍵へのアクセスが許可されていなければ、インターネットから Amazon S3 内のオブジェクトにはアクセスできません。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md	AWS Well-Architected フレームワーク FSI Lens for FISC セキュリティの柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md
実14	-	○	○	AWSネットワークは、既存のネットワークセキュリティの問題に対する強固な保護機能を備えており、お客様はさらに堅牢な保護を実装することができます。 すべての AWS のお客様は、追加料金なしで AWS Shield Standard の保護の適用を自動的に受けることができます。AWS Shield Standard では、ウェブサイトやアプリケーションを標的にした、最も一般的で頻繁に発生するネットワークおよびトランスポートレイヤーの DDoS 攻撃を防御します。AWS Shield Standard を Amazon CloudFront や Amazon Route 53 とともに使用すると、インフラストラクチャ (レイヤー 3 および 4) を標的とした既知の攻撃を総合的に保護できます。 https://aws.amazon.com/jp/shield/ AWS内部では、AWSのネットワークセグメントはISO 27001基準に合わせて作成されています。詳細については、ISO 27001基準の付録A、ドメイン13を参照してください。AWSは、ISO 27001認定基準への対応を確認する独立監査人から、検証および認定を受けています。AWS は、AWS サービスチームおよびセキュリティチームによって決定されるしきい値アラーム生成メカニズムに基づいて、 AWS のモニタリングツールからセキュリティ侵害または潜在的なセキュリティの兆候が示されると、ほぼリアルタイムでアラートします。 論理的または物理的なモニタリングシステムから得られる情報の相関関係を分析し、必要に応じてセキュリティを強化します。 リスクを発見して評価した後、Amazon は、不正行為者の特徴に符合する変則的な使用状況が現れているアカウントを無効にします。	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。 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：リスクとコンプライアンス NIST サイバーセキュリティフレームワーク (CSF) AWS クラウドにおける NIST CSF への準拠 https://d1.awsstatic.com/whitepapers/ja_JP/compliance/NIST_Cybersecurity_Framework_CSF.pdf

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実14	8	-	○	-	ウェブベースのトラフィックの保護を自動化する: AWS では、AWS CloudFormation を使用して、一般的なウェブベースの攻撃をフィルタリングするために設計された AWS WAF ルールセットを自動的にデプロイするソリューションを提供しています。ユーザーは、AWS WAF ウェブアクセスコントロールリスト (ウェブ ACL) に含まれるルールを定義する、あらかじめ設定された保護機能から選択することができます。AWS Partner ソリューションを検討する: AWS パートナーは、お客様のオンプレミス環境にある既存のコントロールと同等または統合された、業界をリードする何百もの製品を提供しています。これらの製品は、既存の AWS サービスを補完し、包括的なセキュリティアーキテクチャの導入と、クラウドとオンプレミス環境におけるよりシームレスなエクスペリエンスを実現します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_network_protection_auto_protect.html Amazon GuardDuty を設定する: GuardDuty は、脅威検出サービスです。悪意のあるアクティビティや不正な動作を継続的にモニタリングし、AWS アカウント とワークロードを保護します。GuardDuty を有効にし、自動アラートを設定します。仮想プライベートクラウド (VPC) フローログを設定する: VPC フローログは、VPC のネットワークインターフェイス間を行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。フローログデータは Amazon CloudWatch Logs および Amazon Simple Storage Service (Amazon S3) にパブリッシュできます。フローログを作成した後、選択した送信先でデータを取得したり表示したりできます。VPC トラフィックのミラーリングを検討する: トラフィックミラーリングは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの Elastic Network Interface からネットワークトラフィックをコピーし、コンテンツ検査、脅威のモニタリング、トラブルシューティングのために帯域外セキュリティおよびモニタリングアプライアンスに送信するために使用できる Amazon VPC の機能です。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_network_protection_inspection.html	AWS Well-Architected フレームワーク セキュリティの柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html
実14	9	-	○	-	ブルートフォース攻撃や不正アクセスを検知するために、ログイン試行回数やログイン履歴などのアプリケーションログを収集します。CloudWatch エージェントや Kinesis エージェントを EC2 にインストールすることで、AWS 上で業務アプリケーションのログを収集することができます。コンテナを実行する場合には、Firelens を用いてログを AWS 上に保存することができます。データベースへのアクセス状況を把握するためには、監査ログが利用できます。 予期されるネットワークトラフィックと予期しないネットワークトラフィックを監視します。不規則なアクセスやネットワークトラフィックを特定します。例えば、ネットワークのメトリクスを監視し、通常時よりも多大なトラフィックが検知される場合は攻撃を受けている可能性があります。予期しない外部システムへの接続の試みは、内部ホストが侵害されている可能性があります。VPC フローログで IP トラフィックに関する情報を記録します。GuardDuty を用いて悪意のある動作や不正な動作を継続的にモニタリングし、AWS のアカウントとワークロードを保護します。AWS Web Application Firewall (WAF) や AWS Shield を用いて外部に公開している Web サイトをサービス妨害攻撃から守ります。AWS WAF では、定義された条件に基づきウェブリクエストを許可、ブロック、監視するルールを設定し、ワークロードを保護します。例えば、レートベースのルールを設定することで、5 分間に一定数以上のリクエストを行った IP アドレスをブロックします。AWS Shield Standard は自動的に有効化され、SYN/UDP フラッド攻撃やリフレクション攻撃といったレイヤー 3 とレイヤー 4 に対する攻撃からワークロードを守ります。 AWS Shield Advances を追加で有効化することで、レイヤー 7 に対する DDoS 攻撃を自動的に緩和します。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md	AWS Well-Architected フレームワーク FSI Lens for FISC セキュリティの柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md
実14	参考5	-	○	-	脆弱性に対する取り組みは以下の通りです。 https://aws.amazon.com/jp/security/vulnerability-reporting/ AWS はセキュリティ情報の形式で公表を行い、AWS セキュリティウェブサイトに掲載いたします。個人や企業、セキュリティ担当チームがよくウェブサイトやフォーラムに各自の勧告を掲載しています。関連性がある場合は、このようなサードパーティのリソースへのリンクも AWS セキュリティ情報に含めています。	

「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	枝番	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	参考6	-	○	-	ペネトレーションテストの AWS カスタマーサポートポリシーは以下の通りです。 https://aws.amazon.com/jp/security/penetration-testing/	
実15	-	○	○	AWSネットワーク管理は、SOC、PCI DSS、ISO 27001、およびFedRAMPsmへのAWSの継続的な準拠の一環として、第三者の独立監査人によって定期的に確認されます。AWSは、そのインフラストラクチャコンポーネントを通じて最小権限を実装しています。また、特定のビジネス目的を持っていないすべてのポートとプロトコルを禁止しています。AWSは、デバイスの使用に不可欠な機能のみの最小実装という厳格な手法に従っています。ネットワークスキャンを実行し、不要なポートまたはプロトコルが使用されている場合は修正されます。AWS環境内のホストオペレーティングシステム、ウェブアプリケーション、およびデータベースでさまざまなツールを利用した、定期的な内外部の脆弱性のスキャンが実行されます。脆弱性のスキャンと解決手法は、AWSのPCI DSSおよびFedRAMPへの継続的な準拠の一環として定期的に確認されます。	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。 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：リスクとコンプライアンス
実15	3	-	○	-	システムへの接続許可を、正当な端末やネットワークを利用して接続する場合のみに与えるよう構成することで、不特定多数の端末からの不正アクセスを防止します。接続元の確認方法としては、認証情報、IP アドレス、クライアント証明書などがあり、これらを組み合わせて利用することでセキュリティを強化できます。 AWS マネジメントコンソールへの API 呼び出しを特定の IP アドレス範囲に限定するには、 一連のアクセス許可がアタッチされた IAM ロール を作成し、aws:SourceIp 条件キーを使用して IAM ロールを引き受けるアクセス許可を IAM ユーザーに付与します。AWS 外のワークロードやアプリケーションなどから AWS の API 呼び出しが必要な場合は、クライアント証明書を利用した一時認証情報の取得を検討します。詳細は IAM Roles Anywhereを参照してください。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md	AWS Well-Architected フレームワーク FSI Lens for FISC セキュリティの柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md
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

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実16	2	-	○	-	Amazon GuardDuty などのツールを使用して、疑わしい活動や定義された境界外にデータを移動させようとする試みを自動的に検出します。例えば、GuardDuty は Amazon Simple Storage Service (Amazon S3) 読み取りアクティビティを検出できますが、それには Exfiltration:S3/AnomalousBehavior 調査結果を使用します.GuardDuty に加えて、ネットワークトラフィック情報をキャプチャする Amazon VPC フローログを Amazon EventBridge とともに使用して、異常な接続 (成功と拒否の両方) の検出をトリガーできます。Amazon S3 Access Analyzer は Amazon S3 バケット内で誰がどのデータにアクセス可能かを評価するのに役立ちます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_data_transit_auto_unintended_access.html	AWS Well-Architected フレームワーク セキュリティの柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html AWS Well-Architected フレームワーク FSI Lens for FISC セキュリティの柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md
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	-	○	○	AWS は、AWS サービスチームおよびセキュリティチームによって決定されるしきい値アラーム生成メカニズムに基づいて、AWS のモニタリングツールからセキュリティ侵害または潜在的なセキュリティの兆候が示されると、ほぼリアルタイムでアラートします。 論理的または物理的なモニタリングシステムから得られる情報の相関関係を分析し、必要に応じてセキュリティを強化します。リスクを発見して評価した後、Amazon は、不正行為者の特徴に符合する変則的な使用状況が現れているアカウントを無効にします。	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。	NIST サイバーセキュリティフレームワーク (CSF) AWS クラウドにおける NIST CSF への準拠 https://d1.awsstatic.com/whitepapers/ja_JP/compliance/NIST_Cybersecurity_Framework_CSF.pdf

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実19	3	-	○	AWS は、文書化された正式なインシデント対応ポリシーとプログラムを実装しています。このポリシーでは、目的、範囲、役割、責任、および管理コミットメントについて取り上げています。AWS は、インシデントの管理に 3 段階の手法を利用しています。 1. アクティブ化および通知段階: AWS のインシデントはイベントの検出で始まります。このソースは、次のように複数あります。a. メトリックスとアラーム - AWS は例外的な状況認識機能を維持しており、ほとんどの問題は 24 時間年中無休のモニタリングと、リアルタイムのメトリックスおよびサービスダッシュボードのアラームにより迅速に検出されます。インシデントの大部分はこのようにして検出されます。 AWS は早期インジケータアラームを利用して、最終的にお客様に影響する可能性のある問題を事前に識別しています。 AWS 従業員が入力したトラブルチケット c. テクニカルホットラインへの 24 時間年中無休の電話による問い合わせ。イベントがインシデント条件を満たす場合、該当するオンコールサポートエンジニアが AWS Event Management Tool システムを利用してエンゲージメントを開始し、該当するプログラムリゾルバー（セキュリティチームなど）を呼び出します。リゾルバーはインシデントの分析を実行して、追加のリゾルバーが必要かどうか判断するとともに、おおよその根本原因を特定します。 2.復旧段階: 該当するリゾルバーが、インシデントに対応する修正策を実行します。トラブルシューティング、修正策、および関連コンポーネントに対応すると、問い合わせリーダーはフォローアップドキュメントとフォローアップアクションの形で次の手順を割り当て、問い合わせエンゲージメントを終了します。 3.再構成段階: 該当する修正アクティビティが完了すると、問い合わせリーダーは復旧段階が完了したことを宣言します。インシデントの事後検証および根本原因の深層分析が該当するチームに割り当てられます。事後分析の結果は該当する上級経営幹部によって確認され、設計変更などの該当するアクションがエラー修正（COE）ドキュメントに記載され、完了まで追跡されます。 上記に示した内部コミュニケーションメカニズムに加えて、 AWS ではその顧客ベースとコミュニティをサポートするために、外部コミュニケーションのさまざまな方法を導入しています。カスタマーエクスペリエンスに影響を与える運用上の問題についてカスタマーサポートチームが通知を受けることができるようにするためのメカニズムが配備されています。 [AWS Health Dashboard] が、顧客サポートチームによって管理運営されており、大きな影響を与える可能性のある問題について顧客に警告を発することができます。AWS のインシデント管理プログラムは、 SOC、 PCI DSS、 ISO 27001、および FedRAMP 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。	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。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。 https://aws.amazon.com/jp/guardduty/ https://aws.amazon.com/jp/detective/	アマゾン ウェブ サービス：リスクとコンプライアンス https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf
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	枝番	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20	3	-	○	-	AWS WAF は、可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性のある一般的なウェブエクスプロイトやボットから保護するのに役立ちます。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。AWS Network Firewall では、ネットワークトラフィックをきめ細かく制御するファイアウォールルールを定義できます。Network Firewall は AWS Firewall Manager と連携するため、Network Firewall ルールに基づいてポリシーを構築し、それらのポリシーを仮想プライベートクラウド (VPC) とアカウント全体に一元的に適用できます。 https://aws.amazon.com/jp/waf/ https://aws.amazon.com/jp/shield/ https://aws.amazon.com/jp/network-firewall/ 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。お客様は Amazon EC2 Auto Scaling を使用することにより、起動テンプレートとして、Amazon マシンイメージ (AMI)、インスタンスタイプ、ブロックストレージデバイス、SSH キーペア、およびインスタンスのインバウンドトラフィックとアウトバウンドトラフィックを制御するセキュリティグループなどのインスタンス属性を設定できます。	アマゾン ウェブ サービス：リスクとコンプライアンス https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf
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

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実21	2	-	○	-	Amazon GuardDuty は、悪意のあるアクティビティのために AWS アカウントとワークロードを継続的にモニタリングし、可視化と修復のための詳細なセキュリティ調査結果を提供する脅威検出サービスです。 Elastic Compute Cloud (EC2) 上で動作するインスタンスとコンテナのワークロードで、マルウェアが疑わしい動作をする可能性のあるファイルを Amazon Elastic Block Store (EBS) でスキャンします。 AWS Security Hub は、 Amazon GuardDuty からの侵入検知結果、 Amazon Inspector からの脆弱性スキャン、および Amazon Macie からの機密データ識別結果などの、AWS アカウント全体で有効化されているセキュリティサービスからの検出結果を収集します。AWS Security Hub は、標準化された AWS Security Finding Format を使用してパートナーのセキュリティ製品からの検出結果を収集するため、時間のかかるデータ解析と正規化の作業が不要になります。お客様は、アカウント全体にわたってあらゆる検出結果を確認できるマスターアカウントを指定できます。 https://aws.amazon.com/jp/guardduty/ https://aws.amazon.com/jp/guardduty/faqs/#GuardDuty_Malware_Protection https://aws.amazon.com/jp/security-hub/ Amazon GuardDuty と AWS Security Hub は、他の AWS のサービスでも利用できるログレコードの集約、重複排除、分析メカニズムを提供します。GuardDuty は、AWS CloudTrail 管理やデータイベント、VPC DNS ログ、および VPC Flow Logs などのソースからの情報を取込み、集計し、分析します。Security Hub は、GuardDuty、AWS Config、Amazon Inspector、Amazon Macie、AWS Firewall Manager、および AWS Marketplace で利用できるかなりの数のサードパーティーセキュリティ製品、そして適切にビルドした場合は独自のコードからの出力を取込み、集計、分析できます。GuardDuty と Security Hub のどちらにも、複数のアカウントにわたって調査結果とインサイトを集約できるマスターメンバーモデルがあります。Security Hub は、オンプレミスの SIEM を導入しているお客様に AWS 側のログ/アラートのプリプロセッサ/アグリゲータとしてよく使用され、お客様はそこから AWS Lambda ベースのプロセッサとフォワーダーを介して Amazon EventBridge を取り込むことができます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_detect_investigate_events_analyze_all.html	AWS Well-Architected フレームワーク セキュリティの柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html
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22	3	-	○	-	Amazon GuardDuty、Amazon EventBridge、および AWS Lambda を使用すると、セキュリティ検出結果に基づいて、自動での修復処置を柔軟に設定できます。たとえば、セキュリティの検出結果に基づいて Lambda 関数を作成し、AWS セキュリティグループのルールを変更できます。GuardDuty の検出結果において、Amazon EC2 インスタンスの 1 つを既知の悪意のある IP が探知したことが示された場合は、EventBridge ルールを使用してそのアドレスを指定できます。このルールは、セキュリティグループルールを自動的に変更し、そのポートへのアクセスを制限する Lambda 関数を起動します。 https://aws.amazon.com/jp/guardduty/faqs/#Enabling_GuardDuty	AWS Well-Architected フレームワーク FSI Lens for FISC セキュリティの柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実23	-	○	○	AWS Information Securityは、COBITフレームワーク、ISO 27001基準、およびPCI DSS要件に基づいて、ポリシーと手続きを規定しています。AWSは、ISO 27001認定基準への対応を確認する独立監査人から、検証および認定を受けています。さらに、AWSはSOC 1 Type IIレポートを発行しています。詳細については、SOC1レポートを参照してください。詳細については、AWSリスクとコンプライアンスホワイトペーパー(http://aws.amazon.com/security)を参照してください。AWSのお客様は、AWSが管理する主な統制を指定できます。主な統制はお客様の統制環境にとって不可欠であり、年次の会計監査などのコンプライアンス要件に準拠するには、その主な統制の運用効率について外部組織による証明が必要です。そのために、AWSは Service Organization Controls 1 (SOC1)TypeIIレポートで幅広く詳細なIT統制を公開しています。SOC1レポートの旧称はStatement on Auditing Standards(SAS)No.70、Service Organizations レポートです。以前はStatement on Standards for Attestation Engagements No.16(SSAE16)レポートと呼ばれ、米国公認会計士協会(AICPA)が作成し、幅広く認められている監査基準です。SOC1監査は、AWSで定義している統制目標および統制活動(AWSが管理するインフラストラクチャの一部に対する統制目標と統制活動が含まれます)の設計と運用効率の両方に関する詳細な監査です。「TypeII」は、レポートに記載されている各統制が、統制の妥当性に関して評価されるだけでなく、運用効率についても外部監査人によるテスト対象であることを示します。AWSの外部監査人は独立し、適格であるため、レポートに記載されている統制は、AWSの統制環境に高い信頼を置けることを示します。	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
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25	3	-	○	-	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。AWS リソースへのアクセスをコントロールするには、IAM コンソール、AWS API、AWS CLI で作成および管理できます。 https://aws.amazon.com/jp/iam/	

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
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。ISO 27001基準に合わせて、すべてのアクセス権付与は定期的に確認されており、明示的な再承認を必須としています。承認しないと、リソースへのアクセスは自動的に失効されます。ユーザーアクセス権の確認に固有の統制については、SOCレポートに概要が記載されています。ユーザー資格の統制の例外については、SOCレポートに記載されています。詳細については、ISO 27001基準の付録A、ドメイン9を参照してください。AWSは、ISO 27001認定基準への対応を確認する独立監査人から、検証および認定を受けています。 従業員の記録がAmazonのヒューマンリソースシステムから削除されると、アクセス権は自動的に取り消されます。従業員の役職に変化が生じる場合、リソースに対するアクセスの継続が明示的に承認される必要があります。そうでない場合、アクセス権は自動的に取り消されます。AWS SOCレポートには、ユーザーアクセスの失効の詳細情報が記載されています。詳細については、ISO 27001基準の付録A、ドメイン9を参照してください。AWSは、ISO 27001認定基準への対応を確認する独立監査人から、検証および認定を受けています。	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27	4	-	○	AWS システムおよびデバイスの承認されたユーザーは、認証されたユーザーのジョブ機能と役割に固有のグループメンバーシップを通じて、アクセス権限が与えられます。グループメンバーシップの条件は、グループ所有者が作成、確認します。ユーザー、グループ、およびシステムアカウントにはすべて一意の IDがあり、再利用されません。ゲスト/匿名および一時アカウントは使用されず、デバイスでは許可されません。ユーザーアカウントは少なくとも四半期ごとに確認されます。四半期ごとに、すべてのグループ所有者は必要に応じて、グループメンバーシップを必要としなくなったユーザーを確認して削除します。この確認は、AWS アカウント管理ツールによってグループ所有者に送信されたシステム通知によって開始されます。この通知では、グループのベースラインを実行するようグループ所有者に伝えます。ベースラインは、グループ所有者によるアクセス権限の完全な再評価です。ベースラインが期限までに完了しない場合、すべてのグループメンバーが削除されます。ユーザーアカウントは、 90 日アクティビティがないとシステムによって自動的に無効になります。AWS は AWS システム内でシステムとデバイス間で監査可能なイベントカテゴリを識別しています。サービスチームは監査機能を設定して、要件に従って継続的にセキュリティ関連イベントを記録しています。ログストレージシステムは、ログストレージの次のニーズが発生すると自動的に容量を増やす、スケーラブルで高可用性のサービスを提供するように設計されています。AWS アクセス管理の手順は、 SOC、 PCI DSS、 ISO 27001、および FedRAMP への AWS の継続的な準拠のために、サードパーティの独立監査人によって確認されます。	保管中のデータを保護するには、分離やバージョニングなどのメカニズムを使ってアクセス制御を実施し、最小特権の原則を適用してください。データへパブリックアクセスが付与されるのを防止します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_data_rest_access_control.html AWS リソースへのアクセス権限付与について、アクセス権限の申請者と承認者で相互牽制が働く構造とすることが推奨されます。IAM エンティティのアクセス許可境界 を利用することで、アイデンティティベースのポリシーが IAM エンティティに付与できるアクセス許可の上限を設定することが可能です。エンティティのアクセス許可の境界により、エンティティは、アイデンティティベースのポリシーとそのアクセス許可の境界の両方で許可されているアクションのみを実行できます。また、特権の昇格を防ぐために、サービスコントロールポリシー (SCP) を利用してアカウント内のユーザー (IAM 管理者または委任された管理者を除く) が管理 IAM アクションを使用できないよう制御することも可能です。アクセス権限は一定期間での見直しが求められますが、それ以外にも、所属や組織の変更に伴う人事異動時、入社や退職、休職、長期の出張、システムの追加やリタイア等のタイミングでも見直しを行うことが必要となります。アクセス権限の見直しは、人に属する権限に限定せず、サーバーリソースに付与されている権限についても見直しが必要です。アクセス権限の管理・変更は、クラウド利用者側でのワークフロー対応の他、AWS Identity and Access Management (IAM) アクセスアドバイザーによる不要なアクセス権限付与の確認や、AWS IAM Access Analyzer による意図しないアクセス許可の確認が有効です。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md	アマゾン ウェブ サービス：リスクとコンプライアンス https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS Well-Architected フレームワーク セキュリティの柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html AWS Well-Architected フレームワーク FSI Lens for FISC セキュリティの柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md
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。	-

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
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。	-
実30	4	-	○	-	AWS Key Management Service (AWS KMS) は、アプリケーションと AWS のサービス全体で暗号キーを作成、管理、制御することができます。 AWS KMS は、暗号化と復号化のための KMS キーを作成する際に 256 ビットのキーをサポートします。発信者に返される生成済みデータキーは、256 ビット、128 ビット、または最大 1024 バイトまでの任意の値にすることができます。AWS KMS でお客様の代わりに 256 ビットの KMS キーを使用して暗号化または復号化を行う場合、Galois Counter Mode の AES アルゴリズム (AES-GCM) が使用されます。カスタマー管理の KMS キーのライフサイクルを管理し、誰がそれを使用または管理できるかを管理します。AWS KMS がキーを自動的にローテーションすることを選択した場合は、データを再暗号化する必要はありません。AWS KMS は過去のバージョンのキーを自動的に保管して、そのキーで暗号化されたデータを復号化できるようにします。AWS KMS のキーに対する新しい暗号化リクエストは、すべて最新バージョンのキーで実行されます。 https://docs.aws.amazon.com/ja_jp/kms/latest/cryptographic-details/crypto-primitives.html	AWS KMS の暗号化の詳細説明 https://docs.aws.amazon.com/ja_jp/kms/latest/cryptographic-details/intro.htmlAWS Well-Architected フレームワーク FSI Lens for FISC セキュリティの柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md
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：リスクとコンプライアンス
実31	4	-	○	-	「AWS の最新情報」 は、すべての AWS 機能、サービス、および発表に関する最新情報を確認する優れた方法です。 https://aws.amazon.com/jp/new/ ナレッジ管理は、チームメンバーが業務を遂行するために情報を検索する際に役立ちます。従業員の学びが促進される組織では、個人を支援する情報が自由に共有されています。情報は探索したり検索したりできます。情報は正確かつ最新の内容です。新しい情報を作成し、既存の情報を更新し、古い情報をアーカイブするメカニズムが存在します。ナレッジ管理プラットフォームの最も一般的な例は、wiki などのコンテンツ管理システムです。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/ops_evolve_ops_knowledge_management.html 運用アクティビティから学んだ教訓を文書化して共有し、社内とチーム全体で利用できるようにします。チームが学んだことを共有して、組織全体のメリットを増やす必要があります。情報とリソースを共有して、回避可能なエラーを防止し、開発作業を容易にする必要があります。これにより、望まれる機能の提供に集中できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/ops_evolve_ops_share_lessons_learned.html	AWS Well-Architected フレームワーク 運用上の優秀性の柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/welcome.html AWSの最新情報 https://aws.amazon.com/jp/new/

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	枝番	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。 AWSセキュリティは、サービスエンドポイントIPアドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします(お客様のインスタンスはこのスキャンの対象外です)。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、脆弱性に対する外部からの脅威の査定が、独立系のセキュリティ会社によって定期的に実行されます。これらの査定に起因する発見や推奨事項は、分類整理されてAWS上層部に報告されます。さらに、AWS統制環境は、通常の内部的および外部的リスク評価によって規定されています。AWSは、外部の認定機関および独立監査人と連携し、AWSの統制環境全体を確認およびテストしています。AWSセキュリティ統制は、SOC、PCI DSS、ISO 27001、およびFedRAMPへの準拠のため、監査中に外部の独立監査人によって確認されます。 AWS は、AWS サービスチームおよびセキュリティチームによって決定されるしきい値アラーム生成メカニズムに基づいて、AWS のモニタリングツールからセキュリティ侵害または潜在的なセキュリティの兆候が示されると、ほぼリアルタイムでアラートします。 論理的または物理的なモニタリングシステムから得られる情報の相関関係を分析し、必要に応じてセキュリティを強化します。リスクを発見して評価した後、Amazon は、不正行為者の特徴に符合する変則的な使用状況が現れているアカウントを無効にします。	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 NIST サイバーセキュリティフレームワーク (CSF) AWS クラウドにおける NIST CSF への準拠 https://d1.awsstatic.com/whitepapers/ja_JP/compliance/NIST_Cybersecurity_Framework_CSF.pdf
実34	4	○	-	AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期 的にスキャンします (お客様のインスタンスはこのスキャンの対象外です)。判明した脆弱性があれば、修正す るために適切な関係者に通知します。さらに、脆弱性に対する外部からの脅威の査定が、独立系のセキュリ ティ会社によって定期的に実行されます。これらの査定に起因する発見や推奨事項は、分類整理されて AWS 上層部に報告されます。これらのスキャンは、基礎となる AWS インフラストラクチャの健全性と可視性を確 認するためのものであり、顧客固有のコンプライアンス要件に適合する必要のある、顧客自身の脆弱性スキャ ンに置き換わることを意味するものではありません。お客様は事前に承認を得た上で、お使いのクラウドインフラストラクチャにスキャンを実施することができますが、対象はお客様のインスタンスに限り、かつ AWS 利用規約に違反しない範囲とします。このようなスキャンについて事前に承認を受けるには、AWS 脆弱性/侵 入テストリクエストフォームを使用してリクエストを送信してください。		アマゾン ウェブ サービス：リスクとコンプライアンス https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
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 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/
実35	2	-	○		サインイン (サインイン認証情報を使った認証) は、多要素認証 (MFA) などのメカニズムを使わない場合、特にサインイン認証情報が不用意に開示されたり、容易に推測されたりする場合に、リスクが発生する恐れがあります。MFA や強力なパスワードポリシーを要求することで、これらのリスクを軽減する強力なサインインのメカニズムを使用します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_identities_enforce_mechanisms.html また、送信元のIPに基づいてAWSへのアクセスを拒否することも可能です。 https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/reference_policies_examples_aws_deny-ip.html これらの機能により、正当なオペレータ以外のアクセスを防止する処置をとってください。	AWS Well-Architected フレームワーク セキュリティの柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html
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

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	枝番	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。 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。	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)
実37	5	-	○	-	AWS CloudTrail は、AWS のサービスアクティビティをキャプチャする AWS アカウント に対して API コールをトラッキングするログサービスです。これは、デフォルトで有効になっており、管理イベントは 90 日間保持され、AWS Management Console、AWS CLI、または AWS を使用して CloudTrail イベント履歴から検索することが可能です。データイベントをより長く保持および確認するには、CloudTrail 証跡を作成して、Amazon S3 バケットと、そしてオプションで Amazon CloudWatch ロググループと関連付けます。または、CloudTrail Lake を作成できます。これは、CloudTrail ログを最長 7 年間保持し、SQL ベースのクエリ施設を提供します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_detect_investigate_events_app_service_logging.html	AWS Well-Architected フレームワーク セキュリティの柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html
実38	-	○	○	AWS の FedRAMP および ISO 27001 認証では、AWS の環境とインフラストラクチャに対するあらゆる変更を運用、維持、制御、承認、デプロイ、レポート、監視するための方針および手順が詳しく記載されています。AWS の物理インフラストラクチャの冗長性と緊急対応をどのように提供しているかについても説明しています。さらに、不正アクセスの防止に向けて、AWS サービスに関するあらゆるリモート保守がどのように承認、実施、記録、審査されているのかが詳しく記載されています。	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。	NIST サイバーセキュリティフレームワーク (CSF) AWS クラウドにおける NIST CSF への準拠 https://d1.awsstatic.com/whitepapers/ja_JP/compliance/NIST_Cybersecurity_Framework_CSF.pdf
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。	-

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実39	5	-	○	-	すべての AWS データストアは、バックアップ機能を備えています。Amazon RDS や Amazon DynamoDB などのサービスは、ポイントインタイムリカバリ (PITR) を有効にする自動バックアップを追加でサポートします。これにより、現在時刻の 5 分前までの任意の時刻にバックアップを復元することができます。 多くの AWS サービスは、バックアップを別の AWS リージョン にコピーする機能を備えています。AWS Backup は、AWS サービス全体にわたるデータ保護を一元化して自動化する機能を提供するツールです。AWS Elastic Disaster Recovery を使用すると、サーバーのワークロード全体をコピーして、オンプレミス、クロス AZ、またはクロスリージョンから継続的なデータ保護を維持できます。目標復旧時点 (RPO) は秒単位で測定されます。Amazon S3 をセルフマネージドおよび AWS マネージドデータソースのバックアップ先として使用できます。 Amazon EBS、Amazon RDS、Amazon DynamoDB などの AWS サービスには、バックアップを作成する機能が組み込まれています。サードパーティー製のバックアップソフトウェアも使用できます。オンプレミスのデータは、AWS Storage Gateway または AWS DataSync を使用して AWS クラウド にバックアップできます。このデータを AWS で保管するには、Amazon S3 バケットを使用できます。 Amazon S3 は、Amazon S3 Glacier や S3 Glacier Deep Archive などの複数のストレージ層を提供し、データストレージコストを低減します。他のソースからデータを再生成することによって、データリカバリのニーズを満たすこともできます。例えば、Amazon ElastiCache レプリカノードまたは Amazon RDS リードレプリカ を使用して、プライマリが失われた場合にデータを再生成できます。 このようなソースを使用して目標復旧時点 (RPO) と目標復旧時間 (RTO) を満たすことができる場合には、バックアップは必要でないことがあります。別の例として、Amazon EMR を使用している場合、データを Amazon S3 から Amazon EMR に再生成できる限り、HDFS データストアをバックアップする必要がないことがあります。バックアップ戦略を選択するときには、データの復旧にかかる時間を考慮してください。データの復旧に必要な時間は、バックアップのタイプ (バックアップ戦略の場合) やデータ再生成メカニズムの複雑性に依存します。この時間は、ワークロードの RTO 以内でなければなりません。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_backing_up_data_identified_backups_data.html	AWS Well-Architected フレームワーク 信頼性の柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/welcome.html
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。	-
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。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。	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。	AWS CSA Consensus Assessments Initiative Questionnaire (CAIQ)
実42	1	-	○	-	インスタンス、コンテナ、サーバーレス機能、またはデバイスで実行されているアプリケーションで動的な構成を使用している場合、 AWS AppConfig を使用して 環境全体での管理と実装を行うことができます。AWS では、 AWS Config を使用して アカウントおよびリージョン全体の AWS リソース構成を 継続的にモニタリングできます。そうすることで、構成履歴の追跡、構成変化の他のリソースへの影響、 AWS Config Rules および AWS Config コンフォーマンスパックを使用した期待される、または望まれる設定との比較監査を行えます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/ops_dev_integ_conf_mgmt_sys.html	AWS Well-Architected フレームワーク 運用上の優秀性の柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/welcome.html

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実42	4	-	○	-	AWS マネジメントコンソールにログインできるユーザーの ID およびパスワードについてはAWS Identity and Access Managementにて管理できます。https://aws.amazon.com/jp/iam/また、AWS マネジメントコンソールへのログイン履歴については AWS CloudTrail に記録されます。 https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-event-reference-aws-console-sign-in-events.html	
実42	参考	-	○	境界保護デバイスは、ルールセット、アクセスコントロールリスト (ACL)、および 設定を使用してネットワークファブリック間で情報の流れを強制する境界保護デバ イスを拒否する deny- all モードで設定されます。 Amazon には複数のネットワークファブリックが存在し、それぞれはファブリック 間の情報の流れを制御するデバイスによって分離されています。ファブリック間の情報の流れは、それらのデバイスにあるアクセスコントロールリスト (ACL) として 存在する承認された機関によって確立されます。これらのデバイスは、ACL の要求 に従ってファブリック間の情報の流れを制御します。ACL は適切な従業員が定義、 承認し、AWS ACL 管理ツールを使用して管理、デプロイされます。 Amazon の情報セキュリティチームがこれらの ACL を承認します。ネットワーク ファブリック間の承認されたファイアウォールルールセットとアクセスコントロー ルリストが、情報の流れを特定の情報システムサービスに制限します。アクセスコ ントロールリストとルールセットは確認、承認され、定期的に (少なくとも 24 時間 ごとに) 境界保護デバイスに自動的にプッシュされて、ルールセットとアクセスコ ントロールリストが最新であることが確認されます。		アマゾン ウェブ サービス：リスクとコンプライアンス https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf
実43	-	○	○	AWSのバックアップおよび冗長性メカニズムは、ISO 27001基準に合わせて開発され、テストされています。AWSのバックアップおよび冗長性メカニズムに関する追加情報については、ISO 27001基準の付録A、ドメイン12およびAWS SOC2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。 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：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	枝番	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43	1	-	○	-	ワークロードモニタリングがどのように実装されているかを頻繁に確認し、重要なイベントや変更に基づいて更新します。効果的なモニタリングは、主要なビジネスメトリクスが原動力になります。ビジネスの優先順位が変化したときに、メトリクスがワークロードに確実に対応できるようにします。 モニタリングを監査することで、アプリケーションがどのタイミングで可用性の目標を満たしているかを確実に把握できます。根本原因の分析には、障害発生時に何が起こったかを発見する機能が必要です。 AWS は、インシデント時にサービスの状態を追跡できるサービスを提供しています。Amazon CloudWatch Logs: このサービスにログを保存してその内容を調査できます。 Amazon CloudWatch Logs Insights: 数秒で大量のログを分析できるフルマネージドサービスです。高速でインタラクティブなクエリと視覚化が行えます。 AWS Config: さまざまな時点でどの AWS インフラストラクチャが使用されているかを確認できます。 AWS CloudTrail: どの AWS API が、いつどのプリンシパルに呼び出されたかを確認できます。AWS では、週に一度のミーティングを実施して、 運用パフォーマンスをレビューし、 学んだ教訓をチーム間で共有しています。AWS には多数のチームが存在するため、 私たちは The Wheel を作成し、 ワークロードをランダムに選んで確認できるようにしました。運用パフォーマンスのレビューと知識の共有を定期的に行うことで、運用チームのパフォーマンスを向上させることができます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_monitor_aws_resources_review_monitoring.html	AWS Well-Architected フレームワーク 信頼性の柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/welcome.html
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
実46	-	○	○	AWS は、自動モニタリングシステムを活用して、ハイレベルなサービスパフォーマンスと可用性を提供します。内部的、外部的両方の使用において、様々なオンラインツールを用いた積極的モニタリングが可能です。AWS 内のシステムには膨大な装置が備わっており、主要なオペレーションメトリックをモニタリングしています。重要計測値が早期警戒しきい値を超える場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。オンコールスケジュールが採用されているので、担当者が運用上の問題にいつでも対応できます。 AWS は、AWS サービスチームおよびセキュリティチームによって決定されるしきい値アラーム生成メカニズムに基づいて、AWS のモニタリングツールからセキュリティ侵害または潜在的なセキュリティの兆候が示されると、ほぼリアルタイムでアラートします。	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 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：AWS リスクとコンプライアンス NIST サイバーセキュリティフレームワーク (CSF) AWS クラウドにおける NIST CSF への準拠 https://d1.awsstatic.com/whitepapers/ja_JP/compliance/NIST_Cybersecurity_Framework_CSF.pdf

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実46	2	-	○	-	ログファイルとメトリクスの履歴を収集し、これらを分析して、幅広いトレンドとワークロードの洞察が得られます。Amazon CloudWatch Logs Insights は、 シンプルかつ強力なクエリ言語をサポートし、 ログデータの分析に使用できます。 Amazon CloudWatch Logs ではさらに、シームレスにデータを Amazon S3 に送ってデータを使用したり、または Amazon Athena に送ってデータをクエリしたりできるサブスクリプションもサポートしています。 豊富な種類のフォーマットのクエリがサポートされています。把握 サポートされる SerDes とデータ形式 詳細については、Amazon Athena ユーザーガイドを参照してください。巨大なログファイルセットの分析では、Amazon EMR クラスターを実行してペタバイト規模の分析を実行できます。 集計、処理、保存、分析を実行できる多数のツールが AWS パートナーやサードパーティによって提供されています。このようなツールには、New Relic、Splunk、Loggly、Logstash、CloudHealth、Nagios などがあります。 ただし、システムやアプリケーションログの外で行うデータ生成は各クラウドプロバイダーに固有であり、また多くの場合サービスごとに固有です。モニタリングプロセスで見落とされがちな点は、データ管理です。モニタリングのためのデータ保存要件を決定し、それに応じたライフサイクルポリシーを適用する必要があります。Amazon S3 はS3 バケットレベルのライフサイクル管理をサポートしています。 このライフサイクル管理には、バケット内のパスごとに異なる管理方法を適用できます。ライフサイクルの最終段階では、データを Amazon S3 Glacier に移行して長期保存し、保存期間の終了後には期限切れにすることができます。S3 Intelligent-Tiering ストレージクラスは、パフォーマンスへの影響や運用のオーバーヘッドなしに、データを最も費用対効果の高いアクセス階層に自動的に移動することにより、コストを最適化できるように設計されています。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_monitor_aws_resources_storage_analytics.html	AWS Well-Architected フレームワーク 信頼性の柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/welcome.html
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 - セキュアな設計 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	枝番	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47	3	-	○	-	AWS Cost Explorerで時間単位の粒度を有効にし、 AWS Cost and Usage Report (CUR)を作成します。これらのデータソースは、組織全体のコストと使用量の最も正確なビューを提供します。CUR では、課金されるすべての AWS のサービスについて、日単位または時間単位の使用量の粒度、料金、コスト、使用属性が提供されます。CUR には、タグ付け、場所、リソース属性、アカウント ID など想定可能なすべてのディメンションがあります。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/cost-optimization-pillar/cost_monitor_usage_detailed_source.html Service Quotas は、250 を超える AWS のサービスのクォータを一元的に管理するのに役立つ AWS のサービスです。クォータ値の検索に加えて、Service Quotas コンソールから、または AWS SDK を使用してクォータ増加をリクエスト、追跡することもできます。AWS Trusted Advisor には、あるサービスの一部の要素に関する使用状況とクォータを表示するサービスクォータチェックが用意されています。サービスごとのデフォルトのサービスクォータは、それぞれのサービスの AWS ドキュメントにも記載されています (例えば、Amazon VPC クォータを参照してください)。スロットルされた API のレート制限など、一部のサービス上の制限は、Amazon API Gateway 内で使用量プランを変更することで設定できます。 それぞれのサービス上の構成として設定される一部の制限には、プロビジョンド IOPS、割り当てられた Amazon RDS ストレージ、Amazon EBS ボリューム割り当てなどがあります。Amazon Elastic Compute Cloud には、インスタンス、Amazon Elastic Block Store、および Elastic IP アドレスの制限を管理するのに役立つ独自のサービスの制限ダッシュボードがあります。サービスクォータがアプリケーションのパフォーマンスに影響を及ぼし、ニーズに合わせて調整できないような事例が発生した場合は、AWS Support に連絡し、緩和策の有無についてお問い合わせください。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_manage_service_limits_aware_quotas_and_constraints.html	AWS Well-Architected フレームワーク 信頼性の柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/welcome.html AWS Well-Architected フレームワーク コスト最適化の柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/cost-optimization-pillar/welcome.html
実47	4	-	○	-	多くの AWS サービスは、需要に合わせて自動的にスケールします。Amazon EC2 インスタンスまたは Amazon ECS クラスターを使用している場合、ワークロードの需要に対応する使用状況のメトリクスに基づいて Auto Scaling を実行するように設定できます。Amazon EC2 では、平均 CPU 使用率、ロードバランサーリクエスト数、またはネットワーク帯域幅を使用して、EC2 インスタンスをスケールアウト (またはスケールイン) できます。Amazon ECS では、平均 CPU 使用率、ロードバランサーリクエスト数、およびメモリ使用率を使用して、ECS タスクをスケールアウト (またはスケールイン) できます。AWS で Target Auto Scaling を使用すると、オートスケーラーは家庭用サーモスタットのように機能し、指定したターゲット値 (例えば、CPU 使用率 70%) を維持するためにリソースを追加または削除します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_adapt_to_changes_proactive_adapt_auto.html	AWS Well-Architected フレームワーク 信頼性の柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/welcome.html
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/

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実48	10	-	○	-	設定を変更し、変更を追跡記録するには、構成管理システムを使用します。これらのシステムは、手動プロセスによって発生するエラーと、変更を導入する労力を減らします。静的な構成管理では、ライフタイムを通じて一貫性を維持することが期待されるリソースの初期化時に値を設定します。このケースの例として、インスタンス上のアプリケーションサーバーまたはウェブサーバー用の構成を設定する場合や、 AWS Management Console 内または AWS CLI を介して AWS サービスの構成を定義する場合が挙げられます。動的な構成管理では、ライフタイムを通じて変化する、または変化することが予測されるリソースの初期化時に値を設定します。例えば、構成変更を介してコードの機能を有効にするように機能トグルを設定したり、インシデント発生時にログの詳細レベルを変更してより多くのデータを取得し、インシデント終了時に詳細レベルを元に戻して不要なログや負荷を減らしたりすることができます。インスタンス、コンテナ、サーバーレス機能、またはデバイスで実行されているアプリケーションで動的な構成を使用している場合、 AWS AppConfig を使用して 環境全体での管理と実装を行うことができます。AWS では、 AWS Config を使用して アカウントおよびリージョン全体の AWS リソース構成を 継続的にモニタリングできます。そうすることで、構成履歴の追跡、構成変化の他のリソースへの影響、 AWS Config Rules および AWS Config コンフォーマンスパックを使用した期待される、または望まれる設定との比較監査を行えます。AWS では、以下のサービスを使用して、継続的インテグレーションと継続的デプロイ (CI/CD) パイプラインを構築できます。 AWS デベロッパーツール (例: AWS CodeCommit、 AWS CodeBuild、 AWS CodePipeline、 AWS CodeDeploy、および AWS CodeStar)。Change Calendar を用意して、変更の実施によって影響を受ける可能性のある重要なビジネスや運用上の活動やイベントが計画されている時期を追跡します。アクティビティを調整して、これらの計画に関するリスクを管理します。 AWS Systems Manager Change Calendar は、変更に対して時間ブロックがオープンであるかクローズであるか、およびその理由を文書化し、 その情報を他の AWS アカウント と共有します。AWS Systems Manager Automation スクリプトは、カレンダーの変化に沿って実行されるように設定できます。AWS Systems Manager メンテナンスウィンドウは、 AWS SSM Run Command または Automation スクリプト、AWS Lambda 呼び出し、または AWS Step Functions アクティビティの実行を指定した時間にスケジュールできます。これらのアクティビティを評価に含めることができるように、Change Calendar 上で印を付けます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/ops_dev_integ_conf_mgmt_sys.html	AWS Well-Architected フレームワーク 運用上の優秀性の柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/welcome.html
実48	11	-	○	-	AWS セキュリティブログは、新しい AWS サービスおよび機能、実装ガイド、および一般的なセキュリティガイダンスを取り上げます。「AWS の最新情報」(http://aws.amazon.com/new)は、すべての AWS 機能、サービス、および発表に関する最新情報を確認する優れた方法です。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_securely_operate_implement_services_features.html	AWSの最新情報 https://aws.amazon.com/jp/new/ AWS Well-Architected フレームワーク セキュリティの柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html
実49	-	○	-	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。	-	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 - セキュアな設定 https://aws.amazon.com/jp/compliance/data-center/controls/
実50	-	○	-	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。	-	アマゾン ウェブ サービス :リスクとコンプライアンス

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	枝番	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
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。 ・データセンターの電力システムは、完全に冗長化され、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。AWS は、施設内の重要かつ不可欠な業務に対応するために、電力障害時に運用を維持するための電力供給を可能とするバックアップ電源がデータセンターに備わっていることを保証しています。 ・AWS データセンターは、環境を制御するとともに、サーバーやその他のハードウェアの適切な運用温度を保ち、過熱を防ぎ、サーバー停止の可能性を減らすためのメカニズムを使用しています。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。 ・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 は、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。	-	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/

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
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
実55	-	○	-	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。	-	AWS Webサイト：AWS のコントロール - セキュアな設計 https://aws.amazon.com/jp/compliance/data-center/controls/#Secure_Design

「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	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定義の論理統制と物理統制の定義は、SOC 1 Type IIレポートに文書化されています。また、このレポートは、この監査チームとコンプライアンスチームのレビューに使用できます。また、AWS ISO 27001およびその他の認定も、監査人のレビュー用に使用できます。物理的セキュリティ統制には、フェンス、壁、保安要員、監視カメラ、侵入検知システムその他の電子的手段による周辺統制が含まれますが、これに限定されるものではありません。物理的アクセスは、建物の周辺および入り口において、監視カメラや侵入検知システムなどの電子的手段を用いる専門の保安要員その他の手段により、厳重に管理されています。権限を付与されたスタッフが2要素認証を最低2回用いて、データセンターのフロアにアクセスします。サーバー設置箇所への物理アクセスポイントは、AWSデータセンター物理セキュリティポリシーの規定により、閉回路テレビ(CCTV)カメラで録画されています。録画は90日間保存されます。ただし、法的または契約義務により30日間に制限される場合もあります。AWSは、このような特権を必要とする正規の業務を有する承認済みの従業員や契約社員に対して、データセンターへの物理的なアクセス権や情報を提供しています。すべての訪問者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが付き添いを行います。物理的なアクセス、データセンターへのアクセスの承認、その他の関連統制については、SOC 1 Type IIレポートを参照してください。 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 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定義の論理統制と物理統制の定義は、SOC 1 Type IIレポートに文書化されています。また、このレポートは、この監査チームとコンプライアンスチームのレビューに使用できます。また、AWS ISO 27001およびその他の認定も、監査人のレビュー用に使用できます。物理的セキュリティ統制には、フェンス、壁、保安要員、監視カメラ、侵入検知システムその他の電子的手段による周辺統制が含まれますが、これに限定されるものではありません。物理的アクセスは、建物の周辺および入り口において、監視カメラや侵入検知システムなどの電子的手段を用いる専門の保安要員その他の手段により、厳重に管理されています。権限を付与されたスタッフが2要素認証を最低2回用いて、データセンターのフロアにアクセスします。サーバー設置箇所への物理アクセスポイントは、AWSデータセンター物理セキュリティポリシーの規定により、閉回路テレビ(CCTV)カメラで録画されています。録画は90日間保存されます。ただし、法的または契約義務により30日間に制限される場合もあります。AWSは、このような特権を必要とする正規の業務を有する承認済みの従業員や契約社員に対して、データセンターへの物理的なアクセス権や情報を提供しています。すべての訪問者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが付き添いを行います。物理的なアクセス、データセンターへのアクセスの承認、その他の関連統制については、SOC 1 Type IIレポートを参照してください。 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 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	枝番	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定義の論理統制と物理統制の定義は、SOC 1 Type IIレポートに文書化されています。また、このレポートは、この監査チームとコンプライアンスチームのレビューに使用できます。また、AWS ISO 27001およびその他の認定も、監査人のレビュー用に使用できます。物理的セキュリティ統制には、フェンス、壁、保安要員、監視カメラ、侵入検知システムその他の電子的手段による周辺統制が含まれますが、これに限定されるものではありません。物理的アクセスは、建物の周辺および入り口において、監視カメラや侵入検知システムなどの電子的手段を用いる専門の保安要員その他の手段により、厳重に管理されています。権限を付与されたスタッフが2要素認証を最低2回用いて、データセンターのフロアにアクセスします。サーバー設置箇所への物理アクセスポイントは、AWSデータセンター物理セキュリティポリシーの規定により、閉回路テレビ(CCTV)カメラで録画されています。録画は90日間保存されます。ただし、法的または契約義務により30日間に制限される場合もあります。AWSは、このような特権を必要とする正規の業務を有する承認済みの従業員や契約社員に対して、データセンターへの物理的なアクセス権や情報を提供しています。すべての訪問者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが付き添いを行います。物理的なアクセス、データセンターへのアクセスの承認、その他の関連統制については、SOC 1 Type IIレポートを参照してください。 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 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/

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	枝番	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	-	○	-	設備のメンテナンス 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。 環境管理 AWS は、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。 CCTV サーバールームに物理的にアクセスできる場所は、閉回路テレビカメラ (CCTV) によって録画されています。画像イメージは、法律およびコンプライアンスに関する要件に従って保持されます。 データセンターのエントリポイント 物理的アクセスは、建物の入り口において、サーベイランスシステム、侵入検知システム、その他の電子的システムを用いて、専門の保安要員によって厳重に管理されています。権限を付与されたスタッフは、多要素認証のメカニズムを利用してデータセンターにアクセスします。サーバールームへの入り口は、ドアがこじ開けられた場合や開け放したままの場合にデバイスでアラームを鳴らし、インシデント対応を開始するように設置された装置で保護されています。 侵入検知 データレイヤー内の場所に電子的手段による進入検出システムが設置され、セキュリティインシデントのモニタリング、検出、および適切な人員への自動的なアラート通知が行われます。サーバールームの入り口および出口は、入場または退場が許可される際に多要素認証を各個人に求める装置で保護されています。これらのデバイスは、許可なくドアがこじ開けられた場合や開け放したままの場合にはアラームを鳴らします。また、ドアのアラームデバイスは、多要素認証を提供せずにデータレイヤーに入場または退場した事例を検出するよう設定されてもいます。アラームは即時のログ記録、分析、および応答のため、24 時間 365 日にわたり AWS セキュリティオペレーションセンターに即時に送信されます。	-	AWS Webサイト：AWS のコントロール - ビジネスの継続性と災害復旧 https://aws.amazon.com/jp/compliance/data-center/controls/
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。	-

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	枝番	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。	-
実70	-	○	○	AWS の従業員は、疑わしいセキュリティインシデントの見分け方と報告先についてトレーニングを受けています。条件に該当する場合は、インシデントが関係機関等に報告されます。AWS は、AWS サービスに影響を及ぼすセキュリティイベントおよびプライバシーイベントをお客様にお知らせする AWS Security Bulletinウェブページを運営しています。Security Bulletin の RSS フィードに登録すると、Security Bulletin ウェブページでの最新のセキュリティ通知を常に把握できます。お客様サポートチームは、可用性に広範な影響を及ぼしている問題についてお客様にアラートを出すサービス状態ダッシュボードのウェブページを運営しています。	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/ ）	NIST サイバーセキュリティフレームワーク (CSF) AWS クラウドにおける NIST CSF への準拠 https://d1.awsstatic.com/whitepapers/ja_JP/compliance/NIST_Cybersecurity_Framework_CSF.pdf
実71	-	○	○	AWS における復元力の高いインフラストラクチャ、信頼性の高い自動化、統制の取れたプロセス、優れた人員を活用すると、お客様の側で処理中断が生じた場合でも、それを最小限に抑え、該当イベントから迅速に復旧できます。AWS の事業継続計画には、AWS のインフラストラクチャの復旧と再構成を目的として開発された、以下の3 フェーズのアプローチが詳しく記載されています。 •アクティベーションと通知のフェーズ •復旧のフェーズ •再構成のフェーズ このアプローチによって、AWS がシステムの復旧と再構成に関する取り組みを体系的な順序で実施することが保証され、取り組みの有効性が最大限に高まり、エラーや作業漏れに起因するシステムの稼働停止時間が最小限に抑えられます。AWS は、すべてのリージョンにわたるユビキタスなセキュリティ制御の環境を維持管理しています。各データセンターは、物理、環境、セキュリティに関する基準に沿ってアクティブ - アクティブ構成として構築されており、n+1 の冗長モデルを採用することによって、コンポーネントに障害が発生した際のシステム可用性を確保しています。コンポーネント(N 個) に対して、少なくとも1 つの独立したバックアップコンポーネント(+1) が配置されており、このバックアップコンポーネントは、運用環境に含まれている他のすべてのコンポーネントが順調に機能している場合もアクティブになります。単一障害点を解消することを目的として、ネットワークとデータセンターの導入を含め、このモデルがAWS 全体で適用されています。すべてのデータセンターがオンラインとなってトラフィックを提供しています。「コールド」状態のデータセンターは存在しません。障害が発生した際も、残りのサイトにトラフィックの負荷を分散できる十分な処理能力が確保されています。 AWS は、インシデント対応に関して、文書化された正式な方針およびプログラムを導入しています。この方針では、目的、範囲、役割、責任、経営者のコミットメントが取り上げられています。AWS は、以下の3 つのフェーズに分かれるインシデント管理アプローチを採用しています。1.アクティベーションと通知のフェーズ2.復旧のフェーズ3.再構成のフェーズAWS のインシデント管理計画から確実な効果が得られるように、AWS はインシデント対応のテストを実施します。このテストでは、その時点の未知の不具合と障害モードについて広い範囲を検出対象としてカバーします。さらに、Amazon のセキュリティチームおよびサービスチームは、お客様への潜在的な影響の有無についてシステムをテストし、検知と分析、封じ込め、除去、復旧、インシデント処理後のアクティビティなど、インシデントの処理に携わる要員を準備することが可能になります。インシデント対応計画と併せて、インシデント対応テスト計画を年1 回作成します。AWS のインシデント管理の計画を作成し、テストを実施し、テスト結果は、第三者の監査人による審査を受けます	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：リスクとコンプライアンス NIST サイバーセキュリティフレームワーク (CSF) AWS クラウドにおける NIST CSF への準拠 https://d1.awsstatic.com/whitepapers/ja_JP/compliance/NIST_Cybersecurity_Framework_CSF.pdf

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実71	4	-	○	-	AWS Health Dashboardでは、AWS サービスの可用性と運用状況を 1 か所で確認できます。AWS サービスの全体的なステータスを表示できます。また、サインインすると、特定の AWS アカウントまたは組織に関するパーソナライズされたコミュニケーションを表示できます。アカウントビューでは、リソースの問題、今後の変更、重要な通知をより詳細に把握できます。 https://docs.aws.amazon.com/ja_jp/health/latest/ug/what-is-aws-health.html AWS またはサードパーティ製のツールを使用して、システムの復旧を自動化し、トラフィックを DR サイトまたはリージョンにルーティングします。設定されたヘルスチェックに基づいて、Elastic Load Balancing や AWS Auto Scaling などの AWS サービスは、正常なアベイラビリティゾーンに負荷を分散できますが、Amazon Route 53、や AWS Global Accelerator などのサービスは、正常な AWS リージョン に負荷をルーティングできます。Route 53 Application Recovery Controller は、準備状況のチェックとルーティングコントロール機能を使用して、フェイルオーバーの管理と調整を支援します。これらの機能は、障害から回復するアプリケーションの能力を継続的にモニタリングするため、複数の AWS リージョン、アベイラビリティゾーン、およびオンプレミスにまたがってアプリケーションの回復を管理できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_planning_for_recovery_auto_recovery.html	AWS Well-Architected フレームワーク 信頼性の柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/welcome.html AWS でのワークロードの災害対策: クラウド内での復旧 https://docs.aws.amazon.com/ja_jp/whitepapers/latest/disaster-recovery-workloads-on-aws/detection.html AWS Health ユーザーガイド https://docs.aws.amazon.com/ja_jp/health/latest/ug/what-is-aws-health.html
実71	5	-	○	-	回避すべきパターンは、まれにしか実行されない復旧経路を作ることです。たとえば、読み取り専用のクエリに使用されるセカンダリデータストアがあるとします。データストアの書き込み時にプライマリデータストアで障害が発生した場合、セカンダリデータストアにフェイルオーバーします。もしこのフェイルオーバーを頻繁にテストしない場合、セカンダリデータストアの機能に関する前提が正しくない可能性があります。セカンダリデータストアの容量は、最後にテストしたときには十分だったかもしれませんが、このシナリオでは負荷に耐えられなくなる可能性があります。エラー復旧がうまくいくのは頻繁にテストする経路のみであることは、これまでの経験からも明らかです。少数の復旧経路を用意することがベストであるのはそのためです。復旧パターンを確立して定期的にテストできます。復旧経路が複雑な場合や重大な場合に復旧経路が正常に機能するという確信を持つには、本番環境でその障害を定期的に実行する必要があります。前述の例では、その必要性に関係なく、スタンバイへのフェイルオーバーを定期的に行う必要があります。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_planning_for_recovery_dr_tested.html AWS Resilience Hub でワークロードの RTO や RPO を含むレジリエンスポリシーを定義することで、構成されるインフラストラクチャやアプリケーション設定などを評価することができます。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/reliability.md	AWS Well-Architected フレームワーク 信頼性の柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/welcome.html AWS Well-Architected フレームワーク FSI Lens for FISC 信頼性の柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/reliability.md

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実72	-	○	○	AWS は、インシデント対応に関して、文書化された正式な方針およびプログラムを導入しています。この方針では、目的、範囲、役割、責任、経営者のコミットメントが取り上げられています。AWS は、以下の3 つのフェーズに分かれるインシデント管理アプローチを採用しています。1.アクティベーションと通知のフェーズ2.復旧のフェーズ3.再構成のフェーズAWS のインシデント管理計画から確実な効果が得られるように、AWS はインシデント対応のテストを実施します。このテストでは、その時点の未知の不具合と障害モードについて広い範囲を検出対象としてカバーします。さらに、Amazon のセキュリティチームおよびサービスチームは、お客様への潜在的な影響の有無についてシステムをテストし、検知と分析、封じ込め、除去、復旧、インシデント処理後のアクティビティなど、インシデントの処理に携わる要員を準備することが可能になります。インシデント対応計画と併せて、インシデント対応テスト計画を年1 回作成します。AWS のインシデント管理の計画を作成し、テストを実施し、テスト結果は、第三者の監査人による審査を受けます。	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/ ）	NIST サイバーセキュリティフレームワーク (CSF) AWS クラウドにおける NIST CSF への準拠 https://d1.awsstatic.com/whitepapers/ja_JP/compliance/NIST_Cybersecurity_Framework_CSF.pdf
実72	8	-	○	-	AWS Health Dashboardでは、AWS サービスの可用性と運用状況を 1 か所で確認できます。AWS サービスの全体的なステータスを表示できます。また、サインインすると、特定の AWS アカウントまたは組織に関するパーソナライズされたコミュニケーションを表示できます。アカウントビューでは、リソースの問題、今後の変更、重要な通知をより詳細に把握できます。 https://docs.aws.amazon.com/ja_jp/health/latest/ug/what-is-aws-health.html	AWS Health ユーザーガイド https://docs.aws.amazon.com/ja_jp/health/latest/ug/what-is-aws-health.html
実72	9	-	○	-	AWS Health Dashboard のサービス履歴では、過去12カ月間のAWSサービスの中断が表示されます。 https://health.aws.amazon.com/health/status	AWS Health Dashboard - サービスの状態 https://health.aws.amazon.com/health/status

「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	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] AWSのビジネス継続性ポリシーおよび計画は、ISO 27001基準に合わせて開発され、テストされています。AWSとビジネス継続性の詳細については、ISO 27001基準の付録A、ドメイン17を参照してください。 [可用性] AWS データセンターは、世界のさまざまなリージョンにクラスター化されて構築されています。すべてのデータセンターはオンラインで顧客にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、影響を受けたエリアから顧客データが移動されます。重要なアプリケーションはN+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。 AWS は、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。各アベイラビリティーゾーンは、独立した障害ゾーンとして設計されています。つまり、アベイラビリティーゾーンは、一般的な都市地域内で物理的に分離されており、洪水の影響が及ばないような場所にあります(洪水地域の分類はリージョンによって異なります)。個別の無停電電源装置(UPS) やオンサイトのバックアップ生成施設に加え、シングルポイントの障害の可能性を減らすために、別々の電力供給施設から異なる配管網を経由して、個別に電力供給を行っています。これらはすべて、冗長的に、複数のTier-1 プロバイダーに接続されています。顧客はAWS の使用量を計画しながら、複数のリージョンやアベイラビリティーゾーンを利用する必要があります。複数のアベイラビリティーゾーンにアプリケーションを配信することによって、自然災害やシステム障害など、ほとんどの障害モードに対して、その可用性を保つことができます。	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：AWS 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	枝番	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73	8	-	○	-	単一の AWS リージョン 内の複数のアベイラビリティゾーン (AZ) にまたがる DR 戦略は、火災、洪水、大規模な停電などの災害イベントに対して影響を緩和できます。ワークロードを特定の AWS リージョン で実行できなくなるような、可能性の低いイベントに対する保護を実装する必要がある場合には、複数のリージョンを使用する DR 戦略を使用できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_planning_for_recovery_disaster_recovery.html	信頼性の柱 - AWS Well-Architected フレームワーク https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/welcome.html
実74	-	○	○	AWS データセンターは、世界のさまざまなリージョンにクラスター化されて構築されています。すべてのデータセンターはオンラインで顧客にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、影響を受けたエリアから顧客データが移動されます。重要なアプリケーションはN+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。 AWS は、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。各アベイラビリティーゾーンは、独立した障害ゾーンとして設計されています。つまり、アベイラビリティーゾーンは、一般的な都市地域内で物理的に分離されており、洪水の影響が及ばないような場所にあります(洪水地域の分類はリージョンによって異なります)。個別の無停電電源装置(UPS) やオンサイトのバックアップ生成施設に加え、シングルポイントの障害の可能性を減らすために、別々の電力供給施設から異なる配管網を経由して、個別に電力供給を行っています。これらはすべて、冗長的に、複数のTier-1 プロバイダーに接続されています。顧客はAWS の使用量を計画しながら、複数のリージョンやアベイラビリティーゾーンを利用する必要があります。複数のアベイラビリティーゾーンにアプリケーションを配信することによって、自然災害やシステム障害など、ほとんどの障害モードに対して、その可用性を保つことができます。	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

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実74	4	-	○	-	単一の AWS リージョン 内の複数のアベイラビリティゾーン (AZ) にまたがる DR 戦略は、火災、洪水、大規模な停電などの災害イベントに対して影響を緩和できます。ワークロードを特定の AWS リージョン で実行できなくなるような、可能性の低いイベントに対する保護を実装する必要がある場合には、複数のリージョンを使用する DR 戦略を使用できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_planning_for_recovery_disaster_recovery.html AWSリージョンやデータセンターの設計を踏まえ、日本における地震災害において、どのようにAWSが高い耐障害性を確保しているか、また、マルチリージョンの活用により、お客様がどのように高いレジリエンスを確保できるかを解説したホワイトペーパーを、AWS Artifactおいて公開しています。 https://aws.amazon.com/jp/blogs/news/resiliency-in-japan/	AWS Well-Architected フレームワーク 信頼性の柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/welcome.html AWS でのワークロードの災害対策: クラウド内での復旧 https://docs.aws.amazon.com/ja_jp/whitepapers/latest/disaster-recovery-workloads-on-aws/detection.html AWSグローバルインフラストラクチャ https://aws.amazon.com/jp/about-aws/global-infrastructure/ AWS Well-Architected フレームワーク FSI Lens for FISC 信頼性の柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/reliability.md
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76	3	-	○	-	AWS では、社内のレポート構造を流用せずに、個別アカウントごとにワークロードを整理し、機能、コンプライアンス要件、共通のコントロールセットに基づいてアカウントをグループ化することを推奨しています。AWS では、アカウントが強固な境界となります。たとえば、開発およびテストのワークロードと本番ワークロードを切り離すために、アカウントレベルの分離を強く推奨しています。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/aws-account-management-and-separation.html	AWS Well-Architected フレームワーク セキュリティの柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html
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	枝番	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82	3	-	○	-	AWS環境における安全なデータ廃棄の方法の例は、以下の記事をご参照ください。 クラウドにおける安全なデータの廃棄 https://aws.amazon.com/jp/blogs/news/data_disposal/ クラウドにおける安全なデータの廃棄（実践編） https://aws.amazon.com/jp/blogs/news/delstoragedatapractice/	クラウドにおける安全なデータの廃棄 https://aws.amazon.com/jp/blogs/news/data_disposal/ クラウドにおける安全なデータの廃棄（実践編） https://aws.amazon.com/jp/blogs/news/delstoragedatapractice/
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	-	○	○	AWS における復元力の高いインフラストラクチャ、信頼性の高い自動化、統制の取れたプロセス、優れた人員を活用すると、お客様の側で処理中断が生じた場合でも、それを最小限に抑え、該当イベントから迅速に復旧できます。AWS の事業継続計画には、AWS のインフラストラクチャの復旧と再構成を目的として開発された、以下の3 フェーズのアプローチが詳しく記載されています。 •アクティベーションと通知のフェーズ •復旧のフェーズ •再構成のフェーズ このアプローチによって、AWS がシステムの復旧と再構成に関する取り組みを体系的な順序で実施することが保証され、取り組みの有効性が最大限に高まり、エラーや作業漏れに起因するシステムの稼働停止時間が最小限に抑えられます。AWS は、すべてのリージョンにわたるユビキタスなセキュリティ制御の環境を維持管理しています。各データセンターは、物理、環境、セキュリティに関する基準に沿ってアクティブ - アクティブ構成として構築されており、n+1 の冗長モデルを採用することによって、コンポーネントに障害が発生した際のシステム可用性を確保しています。コンポーネント(N 個) に対して、少なくとも1 つの独立したバックアップコンポーネント(+1) が配置されており、このバックアップコンポーネントは、運用環境に含まれている他のすべてのコンポーネントが順調に機能している場合もアクティブになります。単一障害点を解消することを目的として、ネットワークとデータセンターの導入を含め、このモデルがAWS 全体で適用されています。すべてのデータセンターがオンラインとなってトラフィックを提供しています。「コールド」状態のデータセンターは存在しません。障害が発生した際も、残りのサイトにトラフィックの負荷を分散できる十分な処理能力が確保されています	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。 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。	NIST サイバーセキュリティフレームワーク (CSF) AWS クラウドにおける NIST CSF への準拠 https://d1.awsstatic.com/whitepapers/ja_JP/compliance/NIST_Cybersecurity_Framework_CSF.pdf

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実85	-	○	○	AWS における復元力の高いインフラストラクチャ、信頼性の高い自動化、統制の取れたプロセス、優れた人員を活用すると、お客様の側で処理中断が生じた場合でも、それを最小限に抑え、該当イベントから迅速に復旧できます。AWS の事業継続計画には、AWS のインフラストラクチャの復旧と再構成を目的として開発された、以下の3 フェーズのアプローチが詳しく記載されています。 •アクティベーションと通知のフェーズ •復旧のフェーズ •再構成のフェーズ このアプローチによって、AWS がシステムの復旧と再構成に関する取り組みを体系的な順序で実施することが保証され、取り組みの有効性が最大限に高まり、エラーや作業漏れに起因するシステムの稼働停止時間が最小限に抑えられます。AWS は、すべてのリージョンにわたるユビキタスなセキュリティ制御の環境を維持管理しています。各データセンターは、物理、環境、セキュリティに関する基準に沿ってアクティブ - アクティブ構成として構築されており、n+1 の冗長モデルを採用することによって、コンポーネントに障害が発生した際のシステム可用性を確保しています。コンポーネント(N 個) に対して、少なくとも1 つの独立したバックアップコンポーネント(+1) が配置されており、このバックアップコンポーネントは、運用環境に含まれている他のすべてのコンポーネントが順調に機能している場合もアクティブになります。単一障害点を解消することを目的として、ネットワークとデータセンターの導入を含め、このモデルがAWS 全体で適用されています。すべてのデータセンターがオンラインとなってトラフィックを提供しています。「コールド」状態のデータセンターは存在しません。障害が発生した際も、残りのサイトにトラフィックの負荷を分散できる十分な処理能力が確保されています。	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。 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。	NIST サイバーセキュリティフレームワーク (CSF) AWS クラウドにおける NIST CSF への準拠 https://d1.awsstatic.com/whitepapers/ja_JP/compliance/NIST_Cybersecurity_Framework_CSF.pdf
実86	-	○	○	AWS における復元力の高いインフラストラクチャ、信頼性の高い自動化、統制の取れたプロセス、優れた人員を活用すると、お客様の側で処理中断が生じた場合でも、それを最小限に抑え、該当イベントから迅速に復旧できます。AWS の事業継続計画には、AWS のインフラストラクチャの復旧と再構成を目的として開発された、以下の3 フェーズのアプローチが詳しく記載されています。 •アクティベーションと通知のフェーズ •復旧のフェーズ •再構成のフェーズ このアプローチによって、AWS がシステムの復旧と再構成に関する取り組みを体系的な順序で実施することが保証され、取り組みの有効性が最大限に高まり、エラーや作業漏れに起因するシステムの稼働停止時間が最小限に抑えられます。AWS は、すべてのリージョンにわたるユビキタスなセキュリティ制御の環境を維持管理しています。各データセンターは、物理、環境、セキュリティに関する基準に沿ってアクティブ - アクティブ構成として構築されており、n+1 の冗長モデルを採用することによって、コンポーネントに障害が発生した際のシステム可用性を確保しています。コンポーネント(N 個) に対して、少なくとも1 つの独立したバックアップコンポーネント(+1) が配置されており、このバックアップコンポーネントは、運用環境に含まれている他のすべてのコンポーネントが順調に機能している場合もアクティブになります。単一障害点を解消することを目的として、ネットワークとデータセンターの導入を含め、このモデルがAWS 全体で適用されています。すべてのデータセンターがオンラインとなってトラフィックを提供しています。「コールド」状態のデータセンターは存在しません。障害が発生した際も、残りのサイトにトラフィックの負荷を分散できる十分な処理能力が確保されています。	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。 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。	NIST サイバーセキュリティフレームワーク (CSF) AWS クラウドにおける NIST CSF への準拠 https://d1.awsstatic.com/whitepapers/ja_JP/compliance/NIST_Cybersecurity_Framework_CSF.pdf
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 リージョン内のすべての AZ は、AZ 間に高スループットかつ低レイテンシーのネットワーキングを提供する、完全に冗長性を持つ専用メトロファイバー上に構築された、高帯域幅、低レイテンシーのネットワーキングで相互接続されています。	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。 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

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
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。	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/ AWS Webサイト：グローバルインフラストラクチャ - リージョンとアベイラビリティーゾーン https://aws.amazon.com/jp/about-aws/global-infrastructure/regions_az/
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。	-
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	枝番	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 における復元力の高いインフラストラクチャ、信頼性の高い自動化、統制の取れたプロセス、優れた人員を活用すると、お客様の側で処理中断が生じた場合でも、それを最小限に抑え、該当イベントから迅速に復旧できます。AWS の事業継続計画には、AWS のインフラストラクチャの復旧と再構成を目的として開発された、以下の3 フェーズのアプローチが詳しく記載されています。 •アクティベーションと通知のフェーズ •復旧のフェーズ •再構成のフェーズ このアプローチによって、AWS がシステムの復旧と再構成に関する取り組みを体系的な順序で実施することが保証され、取り組みの有効性が最大限に高まり、エラーや作業漏れに起因するシステムの稼働停止時間が最小限に抑えられます。 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。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。	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 NIST サイバーセキュリティフレームワーク (CSF) AWS クラウドにおける NIST CSF への準拠 https://d1.awsstatic.com/whitepapers/ja_JP/compliance/NIST_Cybersecurity_Framework_CSF.pdf AWS CSA Consensus Assessments Initiative Questionnaire (CAIQ) 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99	3	-	○	-	ランブックは、特定の成果を達成するために文書化されたプロセスです。ランブックは一連のステップから成り、それをたどることでプロセスを完了できます。ランブックは、飛行機の黎明期から運用に使用されてきました。クラウド運用では、ランブックを使用してリスクを削減し、望ましい成果を達成します。端的に言うと、ランブックはタスクを完了するためのチェックリストです。 ランブックは、組織の成熟度に応じて、いくつかの形態をとります。少なくとも、ステップバイステップのテキスト文書で構成されている必要があります。期待される成果が明確に示されている必要があります。必要な特殊なアクセス許可やツールを明確に文書化します。問題発生時にエラー処理とエスカレーションに関する詳細なガイダンスを提供します。ランブックの所有者をリストアップし、一元的な場所で公開します。ランブックが文書化されたら、チームの別のメンバーに使用してもらって検証します。プロセスの進化につれて、変更管理プロセスに従ってランブックを更新します。 組織が成熟するにつれて、テキストのランブックは自動化されるはずです。例えば、 AWS Systems Manager オートメーションなどのサービスを使用すると、フラットなテキストを、ワークロードに対して実行可能なオートメーションに変換できます。これらのオートメーションはイベントに反応して実行でき、ワークロードを保守する運用上の負担が軽減されます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/ops_ready_to_support_use_runbooks.html 自動スケーリングまたは自動復旧を使用できない場合、または自動復旧が失敗した場合は、AWS Step Functions と AWS Lambda を使用して自動復旧を実装します。自動スケーリングを使用できず、さらに、自動復旧が使用できないか、自動復旧が失敗した場合は、AWS Step Functions と AWS Lambda を使用して修復を自動化できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_withstand_component_failures_auto_healing_system.html	AWS Well-Architected フレームワーク 運用上の優秀性の柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/welcome.html

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実100	-	○	○	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。	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 AWS CSA Consensus Assessments Initiative Questionnaire (CAIQ)
実100	4	-	○	-	AWS には、脆弱性管理プログラムに役立つ様々なサービスがあります。Amazon Inspector は、ソフトウェアの問題と意図しないネットワークアクセスを検出するために、継続的に AWS ワークロードをスキャンします。AWS Systems Manager Patch Manager を使うと、Amazon EC2 インスタンス全体のパッチ適用を管理できます。Amazon Inspector と Systems Manager は、AWS Security Hub で表示できます。これは、AWS セキュリティチェックを自動化して、セキュリティアラートを一元化するのに役立つクラウドセキュリティ体制管理サービスです。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_compute_vulnerability_management.html AWS Config は、設定が誤っているリソースを報告し、AWS Config ポリシーチェックを通して、パブリックアクセスが設定されたリソースを検出できます。AWS Control TowerやAWS Security Hubなどのサービスでは、AWS Organizations 全体でチェックとガードレールのデプロイが簡素化され、公開されたリソースを特定および修復します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_permissions_analyze_cross_account.html	AWS Well-Architected フレームワーク セキュリティの柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html
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/

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実101	3	-	○	-	需要に合わせてリソースをプロアクティブにスケールし、可用性への影響を回避します。 多くの AWS サービスは、需要に合わせて自動的にスケールします。Amazon EC2 インスタンスまたは Amazon ECS クラスターを使用している場合、ワークロードの需要に対応する使用状況のメトリクスに基づいて Auto Scaling を実行するように設定できます。Amazon EC2 では、平均 CPU 使用率、ロードバランサーリクエスト数、またはネットワーク帯域幅を使用して、EC2 インスタンスをスケールアウト (またはスケールイン) できます。Amazon ECS では、平均 CPU 使用率、ロードバランサーリクエスト数、およびメモリ使用率を使用して、ECS タスクをスケールアウト (またはスケールイン) できます。AWS で Target Auto Scaling を使用すると、オートスケーラーは家庭用サーモスタットのように機能し、指定したターゲット値 (例えば、CPU 使用率 70%) を維持するためにリソースを追加または削除します。 AWS Auto Scaling はまた、 Predictive Auto Scaling も実行できます。これは、機械学習を使用して各リソースの過去のワークロードを分析し、次の 2 日間の負荷を定期的に予測します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/design-your-workload-to-adapt-to-changes-in-demand.html	AWS Well-Architected フレームワーク 信頼性の柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/welcome.html
実102	-	○	○	AWS は、自動モニタリングシステムを活用して、ハイレベルなサービスパフォーマンスと可用性を提供します。内部的、外部的両方の使用において、様々なオンラインツールを用いた積極的モニタリングが可能です。AWS 内のシステムには膨大な装置が備わっており、主要なオペレーションメトリックをモニタリングしています。重要計測値が早期警戒しきい値を超える場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。オンコールスケジュールが採用されているので、担当者が運用上の問題にいつでも対応できます。	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：AWS リスクとコンプライアンス
実102	3	-	○	-	ワークロードを設計する際には、可観測性と問題調査への対応においてすべてのコンポーネントにわたって内部状態 (メトリクス、ログ、イベント、トレースなど) を理解するために必要な情報が送出されるようにします。ワークロードの稼働状態を監視し、結果にリスクがあった場合にそれを特定し、効果的な対応を可能にするために必要なテレメトリの開発を繰り返します。AWS ではアプリケーションとワークロードコンポーネントからログ、メトリクス、イベントを送出して収集し、内部的な状況と稼働状態を把握できます。分散トレースを統合して、ワークロードを通過するリクエストを追跡できます。このデータを使用して、アプリケーションと基盤となるコンポーネントがどのように相互作用するかを理解し、問題とパフォーマンスを分析します。ワークロードを計測する際は、フィルターを使用して時間の経過とともに最も有用な情報を選択できるので、状況認識を可能にする幅広い情報 (状態の変化、ユーザーのアクティビティ、権限アクセス、使用量のカウンターなど) を取得します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/design-telemetry.htm lAWS は、Service Health Dashboard でサービスの可用性に関する最新情報を公開しています。いつでも確認して最新のステータス情報を入手したり、RSSフィードを購読して個々のサービスの中断の通知を受けたりすることができます。AWS のいずれかのサービスでリアルタイムの運用上の問題が発生し、それが Service Health Dashboard に表示されない場合は、サポートリクエストを作成できます。AWS Health Dashboard には、アカウントに影響する可能性がある AWS Health イベントの情報が表示されます。情報は 2 つの方法で表示されます。ダッシュボードには、最近のイベントおよび予定されているイベントがカテゴリ別に分類されて表示されます。詳細なイベントログには、過去 90 日間のすべてのイベントが表示されます。 https://docs.aws.amazon.com/ja_jp/whitepapers/latest/disaster-recovery-workloads-on-aws/detection.html	AWS Well-Architected フレームワーク 運用上の優秀性の柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/welcome.html AWS でのワークロードの災害対策: クラウド内での復旧 https://docs.aws.amazon.com/ja_jp/whitepapers/latest/disaster-recovery-workloads-on-aws/detection.html

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
実103	-	○	○	AWS は、自動モニタリングシステムを活用して、ハイレベルなサービスパフォーマンスと可用性を提供します。内部的、外部的両方の使用において、様々なオンラインツールを用いた積極的モニタリングが可能です。AWS 内のシステムには膨大な装置が備わっており、主要なオペレーションメトリックをモニタリングしています。重要計測値が早期警戒しきい値を超える場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。オンコールスケジュールが採用されているので、担当者が運用上の問題にいつでも対応できます。	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：AWS リスクとコンプライアンス
実103	2	-	○	AWS は、AWS クラウド で提供されるすべてのサービスを実行するインフラストラクチャの回復性について責任を負います。このインフラストラクチャは、AWS クラウド サービスを実行するハードウェア、ソフトウェア、ネットワーク、設備で構成されます。AWS は、このような AWS クラウド サービスを利用可能にするうえで商業的に合理的な取り組みを行い、サービスの可用性が AWS サービスレベルアグリーメント (SLA) を満たすか、それ以上を提供することを確認します。AWS グローバルクラウドインフラストラクチャは、お客様が回復力の高いワークロードアーキテクチャを構築できるように設計されています。各 AWS リージョン は完全に分離されており、物理的に分離されたインフラストラクチャのパーティションである複数のアベイラビリティーゾーンで構成されています。アベイラビリティーゾーンは、ワークロードの回復力に影響を及ぼす可能性のある障害を分離し、リージョン内のその他のゾーンへの影響を回避します。ただし同時に、AWS リージョン 内のすべてのゾーンは、高帯域幅、低レイテンシーのネットワークで相互接続されています。ゾーン間をつなぐのは、高スループット、低レイテンシーのネットワークを提供する、完全な冗長性を備えた専用メトロファイバーです。ゾーン間のすべてのトラフィックは暗号化されています。ゾーン間の同期レプリケーションを実行するうえで十分なネットワークパフォーマンスが提供されます。アプリケーションを AZ 間でパーティショニングすると、企業は、停電、落雷、竜巻、台風などの問題から、よりよく隔離され保護されます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/shared-responsibility-model-for-resiliency.html	お客様の責任は、選択した AWS クラウド サービスにより異なります。選択したサービスにより、お客様が回復性についての責任の一環として実行する必要がある設定作業の量が決まります。例えば、Amazon Elastic Compute Cloud (Amazon EC2) のようなサービスでは、お客様は必要となる回復性の設定と管理をすべて実行する必要があります。Amazon EC2 インスタンスをデプロイするお客様の場合は、Amazon EC2 インスタンスを複数のロケーション (AWS アベイラビリティーゾーンなど) にデプロイして、Auto Scaling などのサービスを使用して、自己修復を実装し、インスタンスにインストールしたアプリケーションに対して回復力のあるワークロードアーキテクチャのベストプラクティスを使用する責任があります。Amazon S3 と Amazon DynamoDB などのマネージドサービスの場合は、インフラストラクチャレイヤー、オペレーティングシステム、プラットフォームの運用を AWS が行い、お客様はエンドポイントにアクセスしてデータを保存、取得します。お客様は、バックアップ、バージョニング、レプリケーション戦略など、データの回復力を管理する責任があります。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/shared-responsibility-model-for-resiliency.html リソース障害の発生時に、正常なリソースが引き続きリクエストに対応できるようにします。ロケーション障害 (アベイラビリティゾーンや AWS リージョン など) に対しては、障害のないロケーションの正常なリソースにフェイルオーバーするシステムを用意します。Elastic Load Balancing や AWS Auto Scaling などの AWS のサービスは、複数のリソースおよびアベイラビリティゾーンへの負荷分散に役立ちます。そのため、個々のリソース (EC2 インスタンスなど) の障害や、アベイラビリティゾーンの障害を、残りの正常なリソースにトラフィックをシフトすることによって緩和できます。 マルチリージョンのワークロードの場合、状況はさらに複雑です。例えば、クロスリージョンリードレプリカを使用すると、データを複数の AWS リージョン にデプロイできますが、障害が発生した場合は、リードレプリカをプライマリに昇格させ、そこにトラフィックを向かわせる必要があります。Amazon Route 53 と AWS Global Accelerator は、AWS リージョン 間のトラフィックのルーティングを容易にします。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_withstand_component_failures_failover2good.html	AWS Well-Architected フレームワーク 信頼性の柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/welcome.html
実103-1	-	○	○	対応案にある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。	アマゾン ウェブ サービス：AWS リスクとコンプライアンス
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。	-

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
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	枝番	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。	-

「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	お客様が統制すべき内容	補足情報
		AWS	お客様			
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。	-
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。	-

○ ：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。 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。	-
	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。	-

○ ：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		
	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
- 2022年11月　第10版令和4年7月版の反映、一部情報の更新
- 2023年7月　第11版令和5年5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)	お客様が統制すべき内容(旧)	枝番(新)	AWSの対応状況(新)	お客様が統制すべき内容(新)
実1				5		すべての AWS API と CLI リクエストに対して、長期的認証情報ではなく一時的なセキュリティ認証情報を使用します。AWS サービスに対する API および CLI リクエストは、ほとんどの場合、AWS アクセスキーを使って署名する必要があります。これらのリクエストの署名に使用する認証情報は、一時的でも長期的でもかまいません。長期的認証情報 (長期的アクセスキー) を使用すべき唯一の状況は、IAM ユーザーまたは AWS アカウント ルートユーザーを使用している場合です。AWS に対してフェデレーションを行うか、または他の方法により IAM ロールを担う場合、一時的認証情報が生成されます。サインイン認証情報を使って AWS Management Console にアクセスしても、AWS サービスへのコールを行うために一時的な認証情報が生成されます。長期的認証情報が必要な状況はほとんどなく、一時的な認証情報でほとんどのタスクを遂行できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_identities_unique.html ユーザーが各自のパスワードを変更できるように許可する場合は、強力なパスワードを作成することをユーザーに要求するパスワードポリシーを作成します。 IAM ユーザーのデフォルトのパスワードポリシーでは、次の条件が適用されます。 ・パスワードの文字数制限: 8 ～ 128 文字 ・大文字、小文字、数字、！@ # $ % ^ & * ( ) _ + - = [ ] { } | ' 記号のうち、最低 3 つの文字タイプの組み合わせ ・AWS アカウント名または E メールアドレスと同じでないこと 必要に応じて、IAM コンソールの [Account Settings] (アカウント設定) ページで、AWS アカウントのカスタムパスワードポリシーを作成できます。AWS のデフォルトのパスワードポリシーからアップグレードして、最小文字数、アルファベット以外の文字が必要かどうか、変更頻度など、パスワードの要件を定義します。詳細については、「IAM ユーザー用のアカウントパスワードポリシーの設定」を参照してください。 ID の使用者のみがパスワードを知っている状態を担保するため、ID を発行後、初回サインイン時にパスワードの変更を強制します。IAM ユーザーに初回サインイン時に新しいパスワードの作成を求めるには、AWS マネジメントコンソールの IAM ユーザー作成ウィザードで、[Require password reset (パスワードのリセットが必要)] を選択します。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md
実3	-			8	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。 加えて、詳細についてはAWSクラウドセキュリティホワイトペーパー(http://aws.amazon.com/security で入手可能) を参照してください。 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 認定をセキュリティ保護、配布するために使用されます。 AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。	キーの保存、ローテーション、アクセス制御を含む暗号化アプローチを定義することで、不正ユーザーからのコンテンツの保護や、正規ユーザーへの不必要な公開を防止することができます。AWS Key Management Service (AWS KMS) は暗号化キーの管理をサポートして 多数の AWS のサービスと統合します.このサービスでは、AWS KMS キーのための、耐久性と安全性が高く、冗長なストレージを利用できます。キーのエイリアスのほか、キーレベルのポリシーも定義できます。ポリシーは、キー管理者やキーユーザーを定義するのに役立ちます。さらに、AWS CloudHSM はクラウドベースのハードウェアセキュリティモジュール (HSM) であり、AWS クラウド 上で独自の暗号化キーを簡単に生成して使用できます。FIPS 140-2 レベル 3 検証済みの HSM を使用することで、データセキュリティに関する企業、契約、規制のコンプライアンス要件を満たすことができます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_data_rest_key_mgmt.html

実3	-			参考3		AWS Key Management Service (AWS KMS) は、アプリケーションと AWS のサービス全体で暗号キーを作成、管理、制御することができます。 AWS KMS は、暗号化と復号化のための KMS キーを作成する際に 256 ビットのキーをサポートします。発信者に返される生成済みデータキーは、256 ビット、128 ビット、または最大 1024 バイトまでの任意の値にすることができます。AWS KMS でお客様の代わりに 256 ビットの KMS キーを使用して暗号化または復号化を行う場合、Galois Counter Mode の AES アルゴリズム (AES-GCM) が使用されます。カスタマー管理の KMS キーのライフサイクルを管理し、誰がそれを使用または管理できるかを管理します。AWS KMS がキーを自動的にローテーションすることを選択した場合は、データを再暗号化する必要はありません。AWS KMS は過去のバージョンのキーを自動的に保管して、そのキーで暗号化されたデータを復号化できるようにします。AWS KMS のキーに対する新しい暗号化リクエストは、すべて最新バージョンのキーで実行されます。 https://docs.aws.amazon.com/ja_jp/kms/latest/cryptographic-details/crypto-primitives.html
実4	-			5		暗号化キーと証明書を安全に保存し、厳格なアクセスコントロールによって適切な時間間隔でローテーションします。これを実現する最善の方法として、 AWS Certificate Manager (ACM).これにより、AWS のサービスおよび内部接続リソースで使用するためのパブリックおよびプライベートの Transport Layer Security (TLS) 証明書のプロビジョニング、管理、デプロイが容易になります。TLS 証明書は、ネットワーク通信を保護し、プライベートネットワーク上のリソースだけでなく、インターネット上のウェブサイトのアイデンティティを確立するために使用されます。ACM は、Elastic Load Balancers (ELB)、AWS ディストリビューション、API Gateway の API などの AWS リソース と統合し、証明書の自動更新も処理します。Amazon Elastic Compute Cloud を使用してプライベートルート CA をデプロイする場合、証明書とプライベートキーの両方を ACM (Amazon EC2) インスタンス、コンテナなどで使用するために提供できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_data_transit_key_cert_mgmt.html AWS のサービスには、通信に TLS を使用し、AWS API との通信の際に伝送中データの暗号化を利用できる、HTTPS エンドポイントが用意されています。HTTP など安全でないプロトコルは、セキュリティグループを使用して VPC で監査およびブロックできます。HTTP リクエストは、Amazon CloudFront または Application Load Balancer でHTTPS に自動的にリダイレクトすることもできます。コンピューティングリソースを完全に制御して、サービス全体に伝送中データの暗号化を実装できます。また、外部ネットワークまたは AWS Direct Connect からお使いの VPC に VPN で接続して、トラフィックの暗号化を促進できます。クライアントが AWS API に電話かける際に、最低でも TLS 1.2 を使用していることを確認してください。AWS は、2023 年 6 月に TLS 1.0 と 1.1 の使用を廃止予定です。特別な要件がある場合は、AWS Marketplace でサードパーティーのソリューションを入手できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_data_transit_encrypt.html

実5	-			3		アクセス（最小特権を使用）、分離、バージョニングなど、複数のコントロールによって保管中のデータを保護できます。データへのアクセスは、AWS CloudTrail などの探査メカニズムと、Amazon Simple Storage Service (Amazon S3) アクセスログなどのサービスレベルログを使用して監査する必要があります。パブリックにアクセス可能なデータをインベントリし、時間の経過とともにパブリックで利用可能なデータ量の削減します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_data_rest_access_control.htm IAWS リソースへのアクセス権限について、付与されている権限のうち、利用されていない権限について AWS Identity and Access Management (IAM) アクセスアドバイザーで最終アクセス時間を確認することで検出することが可能になります。アクセス権限の妥当性について確認を行い、不要であれば削除します。インバウンドトラフィックとアウトバウンドトラフィックの両方について、多層防御アプローチでコントロールを適用します。たとえば、Amazon Virtual Private Cloud (VPC) の場合、これにはセキュリティグループ、ネットワーク ACL、サブネットが含まれます。重要なファイルへのアクセスについて、VPC からのみアクセスを許可することで、ネットワークレイヤでの対策を追加することが可能になります。例えば Amazon S3 に保存する場合、VPC エンドポイントやパブリックブロックアクセスを活用することで実現することが可能です。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md
実7	-			2		暗号化キーと証明書を安全に保存し、厳格なアクセスコントロールによって適切な時間間隔でローテーションします。これを実現する最善の方法として、 AWS Certificate Manager (ACM).これにより、AWS のサービスおよび内部接続リソースで使用するためのパブリックおよびプライベートの Transport Layer Security (TLS) 証明書のプロビジョニング、管理、デプロイが容易になります。TLS 証明書は、ネットワーク通信を保護し、プライベートネットワーク上のリソースだけでなく、インターネット上のウェブサイトのアイデンティティを確立するために使用されます。ACM は、Elastic Load Balancers (ELB)、AWS ディストリビューション、API Gateway の API などの AWS リソース と統合し、証明書の自動更新も処理します。Amazon Elastic Compute Cloud を使用してプライベートルート CA をデプロイする場合、証明書とプライベートキーの両方を ACM (Amazon EC2) インスタンス、コンテナなどで使用するために提供できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_data_transit_key_cert_mgmt.htm IAWS のサービスには、通信に TLS を使用し、AWS API との通信の際に伝送中データの暗号化を利用できる、HTTPS エンドポイントが用意されています。HTTP など安全でないプロトコルは、セキュリティグループを使用して VPC で監査およびブロックできます。HTTP リクエストは、Amazon CloudFront または Application Load Balancer でHTTPS に自動的にリダイレクトすることもできます。コンピューティングリソースを完全に制御して、サービス全体に伝送中データの暗号化を実装できます。また、外部ネットワークまたは AWS Direct Connect からお使いの VPC に VPN で接続して、トラフィックの暗号化を促進できます。クライアントが AWS API に電話かける際に、最低でも TLS 1.2 を使用していることを確認してください。AWS は、2023 年 6 月に TLS 1.0 と 1.1 の使用を廃止予定です。特別な要件がある場合は、AWS Marketplace でサードパーティーのソリューションを入手できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_data_transit_encrypt.html

実8	-			7		人的 ID が AWS にサインインする方法は多数あります。AWS ベストプラクティスは、AWS に認証する際にフェデレーション (直接フェデレーションまたは AWS IAM Identity Center (successor to AWS Single Sign-On) を使用) を使って、一元化された ID プロバイダーに依存する方法です。 この場合、ID プロバイダーまたは Microsoft Active Directory を使って、セキュアなサインインプロセスを確立する必要があります。最初に AWS アカウント を開いたとき、AWS アカウント ルートユーザーから始めます。ユーザー (およびルートユーザーを必要とする タスク) へのアクセスを設定するには、アカウントのルートユーザーのみを使用する必要があります。.AWS アカウント を開いた直後にアカウントのルートユーザーに対して MFA を有効化し、AWS ベストプラクティスガイドを使用してルートユーザーをセキュリティ保護することが重要です。AWS IAM Identity Center (successor to AWS Single Sign-On) でユーザーを作成する場合、そのサービスでサインインプロセスをセキュリティ保護します。 消費者アイデンティティについては、Amazon Cognito user pools を使用して、そのサービスで、または Amazon Cognito user pools がサポートする ID プロバイダーの 1 つを使ってサインインプロセスをセキュリティ保護します。AWS Identity and Access Management (IAM) ユーザーを使用している場合、IAM を使ってサインインプロセスをセキュリティ保護することになります。サインイン方法に関係なく、強力なサインインポリシーを適用することが不可欠です。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_identities_enforce_mechanisms.html
実8	-			参考4		すべての AWS API と CLI リクエストに対して、長期的認証情報ではなく一時的なセキュリティ認証情報を使用します。AWS サービスに対する API および CLI リクエストは、ほとんどの場合、AWS アクセスキーを使って署名する必要があります。これらのリクエストの署名に使用する認証情報は、一時的でも長期的でもかまいません。長期的認証情報 (長期的アクセスキー) を使用すべき唯一の状況は、IAM ユーザーまたは AWS アカウント ルートユーザーを使用している場合です。AWS に対してフェデレーションを行うか、または他の方法により IAM ロールを担う場合、一時的認証情報が生成されます。サインイン認証情報を使って AWS Management Console にアクセスしても、AWS サービスへのコールを行うために一時的な認証情報が生成されます。長期的認証情報が必要な状況はほとんどなく、一時的な認証情報ではほとんどのタスクを遂行できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_identities_unique.html
実9	-			2		AWS アカウント を作成する場合は、このアカウントのすべての AWS のサービス とリソースに対して完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることによってアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報を保護し、それらを使用してルートユーザーのみが実行できるタスクを実行します。 https://docs.aws.amazon.com/ja_jp/accounts/latest/reference/root-user.html 以下は、アカウントのルートユーザーを保護するためのベストプラクティスです。 https://docs.aws.amazon.com/ja_jp/accounts/latest/reference/best-practices-root-user.html

実10	-			8		マネジメントコンソールのアクセス履歴はCloudTrailに記録されます。 https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-event-reference-aws-console-sign-in-events.htmlCloudTrail が配信した後で ログファイルが変更、削除、または変更されなかったかどうかを判断するには、CloudTrail ログファイルの整合性の検証を使用することができます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。AWS CLI を使用して CloudTrail が配信した場所のファイルを検証することができます。 https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html
実10	-			9		CloudTrailのイベントは協定世界時(UTC)で出力されます。 https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-event-reference-record-contents.html Amazon では、Amazon Time Sync Service を提供します。このサービスはすべての EC2 インスタンスからアクセスでき、その他の AWS のサービス にも利用されます。このサービスは、各 AWS リージョン で衛星接続された原子基準クロックを使用し、ネットワークタイムプロトコル (NTP) を通じて世界標準時 (UTC) の現在の正確な現在時刻を表示します。Amazon Time Sync Service は、UTC に追加されたうるう秒を自動的に均一化します。 https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/set-time.html すべての Amazon RDS DB インスタンスは、デフォルトで UTC/GMT 時間を使用します。タイムゾーンの変更は任意です。データベースレイヤーでは UTC タイムゾーンを使用するのがベストプラクティスです。UTC では夏時間 (DST) が適用されないため、夏時間の日付となっても時刻を調整する必要はありません。ローカルタイムゾーンを使用する必要がある場合は、代わりにアプリケーションレイヤーでタイムゾーンを変更してください。その際、事前にデータベース管理者またはアプリケーションチームに相談してください。 https://repost.aws/ja/knowledge-center/rds-change-time-zoneCloudWatch ダッシュボードのタイムゾーン形式を変更して、ダッシュボードのデータを UTC またはローカルタイムで表示することもできます。ローカルタイムは、コンピュータのオペレーティングシステムで指定されているタイムゾーンです。 https://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/monitoring/change_dashboard_time_format.html

実10	-			参考2		各アカウントで AWS CloudTrail をオンにして、サポートされている各リージョンで使用します。アクセスが非常に制限されている一元化されたログアカウントに AWS CloudTrail ログを保存します。CloudTrail ログファイルの整合性の検証を使用することでログファイル自体が変更されていないこと、または特定のユーザーの認証情報が特定の API アクティビティを実行したことを確実に検証することができます。 CloudTrail ログファイルの整合性の検証プロセスでは、ログファイルが削除または変更されたかどうかを知ることもできます。また、指定された期間内にログファイルがアカウントに配信されていないことを確実に検証することが可能です。CloudTrail ログファイルを定期的に調べます。 また、AWS CloudTrail イベント、VPC フローログ、DNS ログを継続的に分析することで脅威を検出するサービスである GuardDuty を使用することもできます。Amazon S3 バケットのロギングを有効にして、各バケットに対して行われたリクエストを監視します。アカウントが不正に使用されたと考えられる場合は、発行された一時的な認証情報に注意してください。 認識できない一時的な認証情報が発行された場合は、それらのアクセス許可を無効にします。サービスの最終アクセス時間データを使用して、IAM ロールを定期的に確認します。IAM エンティティ（ユーザーまたはロール）が最後にサービスにアクセスを試みたときのレポートを表示できます。次に、その情報を使用してポリシーを調整し、使用中のサービスのみへのアクセスを許可することができます。IAM のリソースの種類ごとにレポートを生成できます。詳細については、サービスの最終アクセス時間データの表示プロセスのドキュメントをお読みください。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md
実13	-			4	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。 加えて、詳細についてはAWSクラウドセキュリティホワイトペーパー(http://aws.amazon.com/security で入手可能) を参照してください。 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 認定をセキュリティ保護、配布するために使用されます。 AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。	AWS Key Management Service (AWS KMS) は、カスタマーマスターキー (CMK) によるエンベロープ暗号化戦略を採用しています。エンベロープ暗号化は、平文データをデータキーで暗号化し、次にデータキーを別のキー、即ち CMK で暗号化する方法です。AWS KMS の外部でデータの暗号化に利用するデータキーは、CMK により生成、暗号化、復号されています。CMK は AWS KMS で作成され、暗号化されていない状態のままになることはありません。AWS KMS は、カスタマー管理の CMK、AWS 管理の CMK、AWS 所有の CMK という 3 種類の CMK をサポートします (詳細については、 https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys を参照してください)。多くの金融機関のお客様にとって、カスタマー管理の CMK は、お客様のアプリケーションと AWS のサービスの両方からのアクセス権限を管理できるため推奨されます。カスタマー管理の CMK は、キーの生成や保管にさらなる柔軟性も提供します。また、キーの使用またはポリシーの変更はすべて、監査目的で AWS CloudTrail を用いて記録します。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md
実13	-			5		データの暗号化を行う際は、暗号化を行う秘密鍵の管理者とデータを所有するリソースの管理者を分離することでより強固なセキュリティ対策を採用することが可能です。AWS KMS でカスタマーマネージドキーを使用することで、キーポリシーによりアクセス許可を定義することが可能になります。例えば、故意/過失に依らず Amazon S3 内のオブジェクトを不特定多数のインターネットに公開してしまった場合でも、暗号化を行う秘密鍵のキーポリシーでインターネットから秘密鍵へのアクセスが許可されていなければ、インターネットから Amazon S3 内のオブジェクトにはアクセスできません。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md

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		-	AWSネットワークは、既存のネットワークセキュリティの問題に対する強固な保護機能を備えており、お客様はさらに堅牢な保護を実装することができます。 すべての AWS のお客様は、追加料金なしで AWS Shield Standard の保護の適用を自動的に受けることができます。AWS Shield Standard では、ウェブサイトやアプリケーションを標的にした、最も一般的で頻繁に発生するネットワークおよびトランスポートレイヤーの DDoS 攻撃を防御します。AWS Shield Standard を Amazon CloudFront や Amazon Route 53 とともに使用すると、インフラストラクチャ (レイヤー 3 および 4) を標的とした既知の攻撃を総合的に保護できます。 https://aws.amazon.com/jp/shield/ AWS内部では、AWSのネットワークセグメントはISO 27001基準に合わせて作成されています。詳細については、ISO 27001基準の付録A、ドメイン13を参照してください。AWSは、ISO 27001認定基準への対応を確認する独立監査人から、検証および認定を受けています。AWS は、AWS サービスチームおよびセキュリティチームによって決定されるしきい値アラーム生成メカニズムに基づいて、 AWS のモニタリングツールからセキュリティ侵害または潜在的なセキュリティの兆候が示されると、ほぼリアルタイムでアラートします。 論理的または物理的なモニタリングシステムから得られる情報の相関関係を分析し、必要に応じてセキュリティを強化します。リスクを発見して評価した後、Amazon は、不正行為者の特徴に符合する変則的な使用状況が現れているアカウントを無効にします。	
実14	-			8		ウェブベースのトラフィックの保護を自動化する: AWS では、AWS CloudFormation を使用して、一般的なウェブベースの攻撃をフィルタリングするために設計された AWS WAF ルールセットを自動的にデプロイするソリューションを提供しています。ユーザーは、AWS WAF ウェブアクセスコントロールリスト (ウェブ ACL) に含まれるルールを定義する、あらかじめ設定された保護機能から選択することができます。AWS Partner ソリューションを検討する: AWS パートナーは、お客様のオンプレミス環境にある既存のコントロールと同等または統合された、業界をリードする何百もの製品を提供しています。これらの製品は、既存の AWS サービスを補完し、包括的なセキュリティアーキテクチャの導入と、クラウドとオンプレミス環境におけるよりシームレスなエクスペリエンスを実現します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_network_protection_auto_protect.html Amazon GuardDuty を設定する: GuardDuty は、脅威検出サービスです。悪意のあるアクティビティや不正な動作を継続的にモニタリングし、AWS アカウント とワークロードを保護します。GuardDuty を有効にし、自動アラートを設定します。仮想プライベートクラウド (VPC) フローログを設定する: VPC フローログは、VPC のネットワークインターフェイス間を行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。フローログデータは Amazon CloudWatch Logs および Amazon Simple Storage Service (Amazon S3) にパブリッシュできます。フローログを作成した後、選択した送信先でデータを取得したり表示したりできます。VPC トラフィックのミラーリングを検討する: トラフィックミラーリングは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの Elastic Network Interface からネットワークトラフィックをコピーし、コンテンツ検査、脅威のモニタリング、トラブルシューティングのために帯域外セキュリティおよびモニタリングアプライアンスに送信するために使用できる Amazon VPC の機能です。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_network_protection_inspection.html

実14	-			9		ブルートフォース攻撃や不正アクセスを検知するために、ログイン試行回数やログイン履歴などのアプリケーションログを収集します。CloudWatch エージェントや Kinesis エージェントを EC2 にインストールすることで、AWS 上で業務アプリケーションのログを収集することができます。コンテナを実行する場合には、Firelens を用いてログを AWS 上に保存することができます。データベースへのアクセス状況を把握するためには、監査ログが利用できます。 予期されるネットワークトラフィックと予期しないネットワークトラフィックを監視します。不規則なアクセスやネットワークトラフィックを特定します。例えば、ネットワークのメトリクスを監視し、通常時よりも多大なトラフィックが検知される場合は攻撃を受けている可能性があります。予期しない外部システムへの接続の試みは、内部ホストが侵害されている可能性があります。VPC フローログで IP トラフィックに関する情報を記録します。GuardDuty を用いて悪意のある動作や不正な動作を継続的にモニタリングし、AWS のアカウントとワークロードを保護します。AWS Web Application Firewall (WAF) や AWS Shield を用いて外部に公開している Web サイトをサービス妨害攻撃から守ります。AWS WAF では、定義された条件に基づきウェブリクエストを許可、ブロック、監視するルールを設定し、ワークロードを保護します。例えば、レートベースのルールを設定することで、5 分間に一定数以上のリクエストを行った IP アドレスをブロックします。AWS Shield Standard は自動的に有効化され、SYN/UDP フラッド攻撃やリフレクション攻撃といったレイヤー 3 とレイヤー 4 に対する攻撃からワークロードを守ります。AWS Shield Advances を追加で有効化することで、レイヤー 7 に対する DDoS 攻撃を自動的に緩和します。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md
実14	-			参考5		脆弱性に対する取り組みは以下の通りです。 https://aws.amazon.com/jp/security/vulnerability-reporting/ AWS はセキュリティ情報の形式で公表を行い、AWS セキュリティウェブサイトに掲載いたします。個人や企業、セキュリティ担当チームがよくウェブサイトやフォーラムに各自の勧告を掲載しています。関連性がある場合は、このようなサードパーティのリソースへのリンクも AWS セキュリティ情報に含めています。
実14	-			参考6		ペネトレーションテストの AWS カスタマーサポートポリシーは以下の通りです。 https://aws.amazon.com/jp/security/penetration-testing/

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。		-	AWSネットワーク管理は、SOC、PCI DSS、ISO 27001、およびFedRAMPsmへのAWSの継続的な準拠の一環として、第三者の独立監査人によって定期的に確認されます。AWSは、そのインフラストラクチャコンポーネントを通じて最小権限を実装しています。また、特定のビジネス目的を持っていないすべてのポートとプロトコルを禁止しています。AWSは、デバイスの使用に不可欠な機能のみの最小実装という厳格な手法に従っています。ネットワークスキャンを実行し、不要なポートまたはプロトコルが使用されている場合は修正されます。AWS環境内のホストオペレーティングシステム、ウェブアプリケーション、およびデータベースでさまざまなツールを利用した、定期的な内外部の脆弱性のスキャンが実行されます。脆弱性のスキャンと解決手法は、AWSのPCI DSSおよびFedRAMPへの継続的な準拠の一環として定期的に確認されます。	
実15	-			3		システムへの接続許可を、正当な端末やネットワークを利用して接続する場合のみに与えるよう構成することで、不特定多数の端末からの不正アクセスを防止します。接続元の確認方法としては、認証情報、IP アドレス、クライアント証明書などがあり、これらを組み合わせて利用することでセキュリティを強化できます。 AWS マネジメントコンソールへの API 呼び出しを特定の IP アドレス範囲に限定するには、 一連のアクセス許可がアタッチされた IAM ロール を作成し、aws:SourceIp 条件キーを使用して IAM ロールを引き受けるアクセス許可を IAM ユーザーに付与します。AWS 外のワークロードやアプリケーションなどから AWS の API 呼び出しが必要な場合は、クライアント証明書を利用した一時認証情報の取得を検討します。詳細は IAM Roles Anywhereを参照してください。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md
実16	-			2		Amazon GuardDuty などのツールを使用して、疑わしい活動や定義された境界外にデータを移動させようとする試みを自動的に検出します。例えば、GuardDuty は Amazon Simple Storage Service (Amazon S3) 読み取りアクティビティを検出できますが、それには Exfiltration:S3/AnomalousBehavior 調査結果を使用します.GuardDuty に加えて、ネットワークトラフィック情報をキャプチャする Amazon VPC フローログを Amazon EventBridge とともに使用して、異常な接続 (成功と拒否の両方) の検出をトリガーできます。Amazon S3 Access Analyzer は Amazon S3 バケット内で誰がどのデータにアクセス可能かを評価するのに役立ちます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_data_transit_auto_unintended_access.html

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。		-	AWS は、AWS サービスチームおよびセキュリティチームによって決定されるしきい値アラーム生成メカニズムに基づいて、AWS のモニタリングツールからセキュリティ侵害または潜在的なセキュリティの兆候が示されると、ほぼリアルタイムでアラートします。 論理的または物理的なモニタリングシステムから得られる情報の相関関係を分析し、必要に応じてセキュリティを強化します。リスクを発見して評価した後、Amazon は、不正行為者の特徴に符合する変則的な使用状況が現れているアカウントを無効にします。	
実19	-			3	AWS は、文書化された正式なインシデント対応ポリシーとプログラムを実装しています。このポリシーでは、目的、範囲、役割、責任、および管理コミットメントについて取り上げています。AWS は、インシデントの管理に 3 段階の手法を利用しています。 1. アクティブ化および通知段階: AWS のインシデントはイベントの検出で始まります。このソースは、次のように複数あります。a. メトリックスとアラーム - AWS は例外的な状況認識機能を維持しており、ほとんどの問題は 24 時間年中無休のモニタリングと、リアルタイムのメトリックスおよびサービスダッシュボードのアラームにより迅速に検出されます。インシデントの大部分はこのようにして検出されます。 AWS は早期インジケータアラームを利用して、最終的にお客様に影響する可能性のある問題を事前に識別しています。 AWS 従業員が入力したトラブルチケット c. テクニカルホットラインへの 24 時間年中無休の電話による問い合わせ。イベントがインシデント条件を満たす場合、該当するオンコールサポートエンジニアが AWS Event Management Tool システムを利用してエンゲージメントを開始し、該当するプログラムリソルバー（セキュリティチームなど）を呼び出します。リソルバーはインシデントの分析を実行して、追加のリソルバーが必要かどうか判断するとともに、おおよその根本原因を特定します。 2.復旧段階: 該当するリソルバーが、インシデントに対応する修正策を実行します。トラブルシューティング、修正策、および関連コンポーネントに対応すると、問い合わせリーダーはフォローアップドキュメントとフォローアップアクションの形で次の手順を割り当て、問い合わせエンゲージメントを終了します。 3.再構成段階: 該当する修正アクティビティが完了すると、問い合わせリーダーは復旧段階が完了したことを宣言します。インシデントの事後検証および根本原因の深層分析が該当するチームに割り当てられます。事後分析の結果は該当する上級経営幹部によって確認され、設計変更などの該当するアクションがエラー修正（COE）ドキュメントに記載され、完了まで追跡されます。	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。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。 https://aws.amazon.com/jp/guardduty/ https://aws.amazon.com/jp/detective/

					上記に示した内部コミュニケーションメカニズムに加えて、 AWS ではその顧客ベースとコミュニティをサポートするために、外部コミュニケーションのさまざまな方法を導入しています。カスタマーエクスペリエンスに影響を与える運用上の問題についてカスタマーサポートチームが通知を受けることができるようにするためのメカニズムが配備されています。 [AWS Health Dashboard] が、顧客サポートチームによって管理運営されており、大きな影響を与える可能性のある問題について顧客に警告を発することができます。AWS のインシデント管理プログラムは、 SOC、 PCI DSS、 ISO 27001、および FedRAMP 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。	
実20	-			3		AWS WAF は、可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性のある一般的なウェブエクスプロイトやボットから保護するのに役立ちます。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。AWS Network Firewall では、ネットワークトラフィックをきめ細かく制御するファイアウォールルールを定義できます。Network Firewall は AWS Firewall Manager と連携するため、Network Firewall ルールに基づいてポリシーを構築し、それらのポリシーを仮想プライベートクラウド (VPC) とアカウント全体に一元的に適用できます。 https://aws.amazon.com/jp/waf/https://aws.amazon.com/jp/shield/ https://aws.amazon.com/jp/network-firewall/ 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。お客様は Amazon EC2 Auto Scaling を使用することにより、起動テンプレートとして、Amazon マシンイメージ (AMI)、インスタンスタイプ、ブロックストレージデバイス、SSH キーペア、およびインスタンスのインバウンドトラフィックとアウトバウンドトラフィックを制御するセキュリティグループなどのインスタンス属性を設定できます。

実21	-			2		Amazon GuardDuty は、悪意のあるアクティビティのために AWS アカウントとワークロードを継続的にモニタリングし、可視化と修復のための詳細なセキュリティ調査結果を提供する脅威検出サービスです。 Elastic Compute Cloud (EC2) 上で動作するインスタンスとコンテナのワークロードで、マルウェアが疑わしい動作をする可能性のあるファイルを Amazon Elastic Block Store (EBS) でスキャンします。 AWS Security Hub は、Amazon GuardDuty からの侵入検知結果、 Amazon Inspector からの脆弱性スキャン、および Amazon Macie からの機密データ識別結果などの、AWS アカウント全体で有効化されているセキュリティサービスからの検出結果を収集します。AWS Security Hub は、標準化された AWS Security Finding Format を使用してパートナーのセキュリティ製品からの検出結果を収集するため、時間のかかるデータ解析と正規化の作業が不要になります。お客様は、アカウント全体にわたってあらゆる検出結果を確認できるマスターアカウントを指定できます。 https://aws.amazon.com/jp/guardduty/ https://aws.amazon.com/jp/guardduty/faqs/#GuardDuty_Malware_Protection https://aws.amazon.com/jp/security-hub/ Amazon GuardDuty と AWS Security Hub は、他の AWS のサービスでも利用できるログレコードの集約、重複排除、分析メカニズムを提供します。GuardDuty は、AWS CloudTrail 管理やデータイベント、VPC DNS ログ、および VPC Flow Logs などのソースからの情報を取込み、集計し、分析します。Security Hub は、GuardDuty、AWS Config、Amazon Inspector、Amazon Macie、AWS Firewall Manager、および AWS Marketplace で利用できるかなりの数のサードパーティーセキュリティ製品、そして適切にビルドした場合は独自のコードからの出力を取込み、集計、分析できます。GuardDuty と Security Hub のどちらにも、複数のアカウントにわたって調査結果とインサイトを集約できるマスターメンバーモデルがあります。Security Hub は、オンプレミスの SIEM を導入しているお客様に AWS 側のログ/アラートのプリプロセッサ/アグリゲータとしてよく使用され、お客様はそこから AWS Lambda ベースのプロセッサとフォワーダーを介して Amazon EventBridge を取り込むことができます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_detect_investigate_events_analyze_all.html
実22	-			3		Amazon GuardDuty、Amazon EventBridge、および AWS Lambda を使用すると、セキュリティ検出結果に基づいて、自動での修復処置を柔軟に設定できます。たとえば、セキュリティの検出結果に基づいて Lambda 関数を作成し、AWS セキュリティグループのルールを変更できます。GuardDuty の検出結果において、Amazon EC2 インスタンスの 1 つを既知の悪意のある IP が探知したことが示された場合は、EventBridge ルールを使用してそのアドレスを指定できます。このルールは、セキュリティグループルールを自動的に変更し、そのポートへのアクセスを制限する Lambda 関数を起動します。 https://aws.amazon.com/jp/guardduty/faqs/#Enabling_GuardDuty

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。		-	AWS Information Securityは、COBITフレームワーク、ISO 27001基準、およびPCI DSS要件に基づいて、ポリシーと手続きを規定しています。AWSは、ISO 27001認定基準への対応を確認する独立監査人から、検証および認定を受けています。さらに、AWSはSOC 1 Type IIレポートを発行しています。詳細については、SOC1レポートを参照してください。詳細については、AWSリスクとコンプライアンスホワイトペーパー (http://aws.amazon.com/security)を参照してください。AWSのお客様は、AWSが管理する主な統制を指定できます。主な統制はお客様の統制環境にとって不可欠であり、年次の会計監査などのコンプライアンス要件に準拠するには、その主な統制の運用効率について外部組織による証明が必要です。そのために、AWSは Service Organization Controls 1 (SOC1)TypeIIレポートで幅広く詳細なIT統制を公開しています。SOC1レポートの旧称はStatement on Auditing Standards(SAS)No.70、Service Organizations レポートです。以前はStatement on Standards for Attestation Engagements No.16(SSAE16)レポートと呼ばれ、米国公認会計士協会(AICPA)が作成し、幅広く認められている監査基準です。SOC1監査は、AWSで定義している統制目標および統制活動(AWSが管理するインフラストラクチャの一部に対する統制目標と統制活動が含まれます)の設計と運用効率の両方に関する詳細な監査です。「TypeII」は、レポートに記載されている各統制が、統制の妥当性に関して評価されるだけでなく、運用効率についても外部監査人によるテスト対象であることを示します。AWSの外部監査人は独立し、適格であるため、レポートに記載されている統制は、AWSの統制環境に高い信頼を置けることを示します。	
実25	-			3		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。AWS リソースへのアクセスをコントロールするには、IAM コンソール、AWS API、AWS CLI で作成および管理できます。 https://aws.amazon.com/jp/iam/
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。		-	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。 ISO 27001基準に合わせて、すべてのアクセス権付与は定期的に確認されており、明示的な再承認を必須としています。承認しないと、リソースへのアクセスは自動的に失効されます。ユーザーアクセス権の確認に固有の統制については、SOCレポートに概要が記載されています。ユーザー資格の統制の例外については、SOCレポートに記載されています。詳細については、ISO 27001基準の付録A、ドメイン9を参照してください。AWSは、ISO 27001認定基準への対応を確認する独立監査人から、検証および認定を受けています。 従業員の記録がAmazonのヒューマンリソースシステムから削除されると、アクセス権は自動的に取り消されます。従業員の役職に変化が生じる場合、リソースに対するアクセスの継続が明示的に承認される必要があります。そうでない場合、アクセス権は自動的に取り消されます。AWS SOCレポートには、ユーザーアクセスの失効の詳細情報が記載されています。詳細については、ISO 27001基準の付録A、ドメイン9を参照してください。AWSは、ISO 27001認定基準への対応を確認する独立監査人から、検証および認定を受けています。	

実27	-			4	AWS システムおよびデバイスの承認されたユーザーは、認証されたユーザーのジョブ機能と役割に固有のグループメンバーシップを通じて、アクセス権限が与えられます。グループメンバーシップの条件は、グループ所有者が作成、確認します。ユーザー、グループ、およびシステムアカウントにはすべて一意の IDがあり、再利用されません。ゲスト/匿名および一時アカウントは使用されず、デバイスでは許可されません。ユーザーアカウントは少なくとも四半期ごとに確認されます。四半期ごとに、すべてのグループ所有者は必要に応じて、グループメンバーシップを必要としなくなったユーザーを確認して削除します。この確認は、AWS アカウント管理ツールによってグループ所有者に送信されたシステム通知によって開始されます。この通知では、グループのベースラインを実行するようグループ所有者に伝えます。ベースラインは、グループ所有者によるアクセス権限の完全な再評価です。ベースラインが期限までに完了しない場合、すべてのグループメンバーが削除されます。ユーザーアカウントは、 90 日アクティビティがないとシステムによって自動的に無効になります。AWS は AWS システム内でシステムとデバイス間で監査可能なイベントカテゴリを識別しています。サービスチームは監査機能を設定して、要件に従って継続的にセキュリティ関連イベントを記録しています。ログストレージシステムは、ログストレージの次のニーズが発生すると自動的に容量を増やす、スケーラブルで高可用性のサービスを提供するように設計されています。AWS アクセス管理の手順は、 SOC、 PCI DSS、 ISO 27001、および FedRAMP への AWS の継続的な準拠のために、サードパーティの独立監査人によって確認されます。	保管中のデータを保護するには、分離やパージョニングなどのメカニズムを使ってアクセス制御を実施し、最小特権の原則を適用してください。データへパブリックアクセスが付与されるのを防止します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_data_rest_access_control.html AWS リソースへのアクセス権限付与について、アクセス権限の申請者と承認者で相互牽制が働く構造とすることが推奨されます。IAM エンティティのアクセス許可境界 を利用することで、アイデンティティベースのポリシーが IAM エンティティに付与できるアクセス許可の上限を設定することが可能です。エンティティのアクセス許可の境界により、エンティティは、アイデンティティベースのポリシーとそのアクセス許可の境界の両方で許可されているアクションのみを実行できます。また、特権の昇格を防ぐために、サービスコントロールポリシー (SCP) を利用してアカウント内のユーザー (IAM 管理者または委任された管理者を除く) が管理 IAM アクションを使用できないよう制御することも可能です。アクセス権限は一定期間での見直しが求められますが、それ以外にも、所属や組織の変更に伴う人事異動時、入社や退職、休職、長期の出張、システムの追加やリタイア等のタイミングでも見直しを行うことが必要となります。アクセス権限の見直しは、人に属する権限に限定せず、サーバーリソースに付与されている権限についても見直しが必要です。アクセス権限の管理・変更は、クラウド利用者側でのワークフロー対応の他、AWS Identity and Access Management (IAM) アクセスアドバイザーによる不要なアクセス権限付与の確認や、AWS IAM Access Analyzer による意図しないアクセス許可の確認が有効です。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md
実30	-			4		AWS Key Management Service (AWS KMS) は、アプリケーションと AWS のサービス全体で暗号キーを作成、管理、制御することができます。 AWS KMS は、暗号化と復号化のための KMS キーを作成する際に 256 ビットのキーをサポートします。発信者に返される生成済みデータキーは、256 ビット、128 ビット、または最大 1024 バイトまでの任意の値にすることができます。AWS KMS でお客様の代わりに 256 ビットの KMS キーを使用して暗号化または復号化を行う場合、Galois Counter Mode の AES アルゴリズム (AES-GCM) が使用されます。カスタマー管理の KMS キーのライフサイクルを管理し、誰がそれを使用または管理できるかを管理します。AWS KMS がキーを自動的にローテーションすることを選択した場合は、データを再暗号化する必要はありません。AWS KMS は過去のバージョンのキーを自動的に保管して、そのキーで暗号化されたデータを復号化できるようにします。AWS KMS のキーに対する新しい暗号化リクエストは、すべて最新バージョンのキーで実行されます。 https://docs.aws.amazon.com/ja_jp/kms/latest/cryptographic-details/crypto-primitives.html

実31	-			4		「AWS の最新情報」 は、すべての AWS 機能、サービス、および発表に関する最新情報を確認する優れた方法です。 https://aws.amazon.com/jp/new/ ナレッジ管理は、チームメンバーが業務を遂行するために情報を検索する際に役立ちます。従業員の学びが促進される組織では、個人を支援する情報が自由に共有されています。情報は探索したり検索したりできます。情報は正確かつ最新の内容です。新しい情報を作成し、既存の情報を更新し、古い情報をアーカイブするメカニズムが存在します。ナレッジ管理プラットフォームの最も一般的な例は、wiki などのコンテンツ管理システムです。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/ops_evolve_ops_knowledge_management.html 運用アクティビティから学んだ教訓を文書化して共有し、社内とチーム全体で利用できるようにします。チームが学んだことを共有して、組織全体のメリットを増やす必要があります。情報とリソースを共有して、回避可能なエラーを防止し、開発作業を容易にする必要があります。これにより、望まれる機能の提供に集中できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/ops_evolve_ops_share_lessons_learned.html
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。		-	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。 AWSセキュリティは、サービスエンドポイントIPアドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします(お客様のインスタンスはこのスキャンの対象外です)。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、脆弱性に対する外部からの脅威の査定が、独立系のセキュリティ会社によって定期的に実行されます。これらの査定に起因する発見や推奨事項は、分類整理されてAWS上層部に報告されます。 さらに、AWS統制環境は、通常の内部的および外部的リスク評価によって規定されています。AWSは、外部の認定機関および独立監査人と連携し、AWSの統制環境全体を確認およびテストしています。AWSセキュリティ統制は、SOC、PCI DSS、ISO 27001、およびFedRAMPへの準拠のため、監査中に外部の独立監査人によって確認されます。 AWS は、AWS サービスチームおよびセキュリティチームによって決定されるしきい値アラーム生成メカニズムに基づいて、AWS のモニタリングツールからセキュリティ侵害または潜在的なセキュリティの兆候が示されると、ほぼリアルタイムでアラートします。 論理的または物理的なモニタリングシステムから得られる情報の相関関係を分析し、必要に応じてセキュリティを強化します。リスクを発見して評価した後、Amazon は、不正行為者の特徴に符合する変則的な使用状況が現れているアカウントを無効にします。	

実34	-			4	AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期 的にスキャンします (お客様のインスタンスはこのスキャンの対象外です)。判明した脆弱性があれば、修正す るために適切な関係者に通知します。さらに、脆弱性に対する外部からの脅威の査定が、独立系のセキュリ ティ会社によって定期的に実行されます。これらの査定に起因する発見や推奨事項は、分類整理されて AWS 上層部に報告されます。これらのスキャンは、基礎となる AWS インフラストラクチャの健全性と可視性を確 認するためのものであり、顧客固有のコンプライアンス要件に適合する必要のある、顧客自身の脆弱性スキャ ンに置き換わることを意味するものではありません。お客様は事前に承認を得た上で、お使いのクラウドイン フラストラクチャにスキャンを実施することができますが、対象はお客様のインスタンスに限り、かつ AWS 利用規約に違反しない範囲とします。このようなスキャンについて事前に承認を受けるには、AWS 脆弱性/侵 入テストリクエストフォームを使用してリクエストを送信してください。	
実35	-			2		サインイン (サインイン認証情報を使った認証) は、多要素認証 (MFA) などのメカニズムを使わない場合、特にサインイン認証情報が不用意に開示されたり、容易に推測されたりする場合に、リスクが発生する恐れがあります。MFA や強力なパスワードポリシーを要求することで、これらのリスクを軽減する強力なサインインのメカニズムを使用します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_identities_enforce_mechanisms.html また、送信元のIPに基づいてAWSへのアクセスを拒否することも可能です。 https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/reference_policies_examples_aws_deny-ip.html これらの機能により、正当なオペレータ以外のアクセスを防止する処置をとってください。
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。		-	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。	

実37	-			5		AWS CloudTrail は、AWS のサービスアクティビティをキャプチャする AWS アカウント に対して API コールをトラッキングするログサービスです。これは、デフォルトで有効になっており、管理イベントは 90 日間保持され、AWS Management Console、AWS CLI、または AWS を使用して CloudTrail イベント履歴から検索することが可能です。データイベントをより長く保持および確認するには、CloudTrail 証跡を作成して、Amazon S3 バケットと、そしてオプションで Amazon CloudWatch ロググループと関連付けます。または、CloudTrail Lake を作成できます。これは、CloudTrail ログを最長 7 年間保持し、SQL ベースのクエリ施設を提供します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_detect_investigate_events_app_service_logging.html
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		-	AWS の FedRAMP および ISO 27001 認証では、AWS の環境とインフラストラクチャに対するあらゆる変更を連用、維持、制御、承認、デプロイ、レポート、監視するための方針および手順が詳しく記載されています。AWS の物理インフラストラクチャの冗長性と緊急対応をどのように提供しているかについても説明しています。さらに、不正アクセスの防止に向けて、AWS サービスに関するあらゆるリモート保守がどのように承認、実施、記録、審査されているのかが詳しく記載されています。	
実39	-			5		すべての AWS データストアは、バックアップ機能を備えています。Amazon RDS や Amazon DynamoDB などのサービスは、ポイントインタイムリカバリ (PITR) を有効にする自動バックアップを追加でサポートします。これにより、現在時刻の 5 分前までの任意の時刻にバックアップを復元することができます。 多くの AWS サービスは、バックアップを別の AWS リージョン にコピーする機能を備えています。AWS Backup は、AWS サービス全体にわたるデータ保護を一元化して自動化する機能を提供するツールです。AWS Elastic Disaster Recovery を使用すると、サーバーのワークロード全体をコピーして、オンプレミス、クロス AZ、またはクロスリージョンから継続的なデータ保護を維持できます。目標復旧時点 (RPO) は秒単位で測定されます。 Amazon S3 をセルフマネージドおよび AWS マネージドデータソースのバックアップ先として使用できます。 Amazon EBS、Amazon RDS、Amazon DynamoDB などの AWS サービスには、バックアップを作成する機能が組み込まれています。サードパーティー製のバックアップソフトウェアも使用できます。オンプレミスのデータは、AWS Storage Gateway または AWS DataSync を使用して AWS クラウド にバックアップできます。このデータを AWS で保管するには、Amazon S3 バケットを使用できます。 Amazon S3 は、Amazon S3 Glacier や S3 Glacier Deep Archive などの複数のストレージ層を提供し、データストレージコストを低減します。他のソースからデータを再生成することによって、データリカバリのニーズを満たすこともできます。例えば、Amazon ElastiCache レプリカノードまたは Amazon RDS リードレプリカ を使用して、プライマリが失われた場合にデータを再生成できます。 このようなソースを使用して目標復旧時点 (RPO) と目標復旧時間 (RTO) を満たすことができる場合には、バックアップは必要でないことがあります。別の例として、Amazon EMR を使用している場合、データを Amazon S3 から Amazon EMR に再生成できる限り、HDFS データストアをバックアップする必要がないことがあります。 バックアップ戦略を選択するときには、データの復旧にかかる時間を考慮してください。データの復旧に必要な時間は、バックアップのタイプ (バックアップ戦略の場合) やデータ再生成メカニズムの複雑性に依存します。この時間は、ワークロードの RTO 以内でなければなりません。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_backing_up_data_identified_backups_data.html

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。		-	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。	
実42	-			1		インスタンス、コンテナ、サーバーレス機能、またはデバイスで実行されているアプリケーションで動的な構成を使用している場合、 AWS AppConfig を使用して 環境全体での管理と実装を行うことができます。AWS では、AWS Config を使用して アカウントおよびリージョン全体の AWS リソース構成を 継続的にモニタリングできます。そうすることで、構成履歴の追跡、構成変化の他のリソースへの影響、 AWS Config Rules および AWS Config コンフォーマンスパックを使用した期待される、または望まれる設定との比較監査を行えます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/ops_dev_integ_conf_mgmt_sys.html
実42	-			4		AWS マネジメントコンソールにログインできるユーザーの ID およびパスワードについてはAWS Identity and Access Managementにて管理できます。https://aws.amazon.com/jp/iam/また、AWS マネジメントコンソールへのログイン履歴については AWS CloudTrail に記録されます。 https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-event-reference-aws-console-sign-in-events.html
実42	-			参考	境界保護デバイスは、ルールセット、アクセスコントロールリスト (ACL)、および 設定を使用してネットワークファブリック間で情報の流れを強制する境界保護デバ イスを拒否する deny- all モードで設定されます。 Amazon には複数のネットワークファブリックが存在し、それぞれはファブリック 間の情報の流れを制御するデバイスによって分離されています。ファブリック間の 情報の流れは、それらのデバイスにあるアクセスコントロールリスト (ACL) として 存在する承認された機関によって確立されます。これらのデバイスは、ACL の要求 に従ってファブリック間の情報の流れを制御します。ACL は適切な従業員が定義、 承認し、AWS ACL 管理ツールを使用して管理、デプロイされます。 Amazon の情報セキュリティチームがこれらの ACL を承認します。ネットワークファブリック間の承認されたファイアウォールルールセットとアクセスコントロー ルリストが、情報の流れを特定の情報システムサービスに制限します。アクセスコ ントロールリストとルールセットは確認、承認され、定期的に (少なくとも 24 時間 ごとに) 境界保護デバイスに自動的にプッシュされて、ルールセットとアクセスコ ントールリストが最新であることが確認されます。	

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。		-	AWSのバックアップおよび冗長性メカニズムは、ISO 27001基準に合わせて開発され、テストされています。AWSのバックアップおよび冗長性メカニズムに関する追加情報については、ISO 27001基準の付録A、ドメイン12およびAWS SOC2レポートを参照してください。	
実43	-			1		ワークロードモニタリングがどのように実装されているかを頻繁に確認し、重要なイベントや変更に基づいて更新します。効果的なモニタリングは、主要なビジネスメトリクスが原動力になります。ビジネスの優先順位が変化したときに、メトリクスがワークロードに確実に対応できるようにします。 モニタリングを監査することで、アプリケーションがどのタイミングで可用性の目標を満たしているかを確実に把握できます。根本原因の分析には、障害発生時に何が起こったかを発見する機能が必要です。 AWS は、インシデント時にサービスの状態を追跡できるサービスを提供しています。Amazon CloudWatch Logs: このサービスにログを保存してその内容を調査できます。 Amazon CloudWatch Logs Insights: 数秒で大量のログを分析できるフルマネージドサービスです。高速でインタラクティブなクエリと視覚化が行えます。 AWS Config: さまざまな時点でどの AWS インフラストラクチャが使用されているかを確認できます。 AWS CloudTrail: どの AWS API が、いつどのプリンシパルに呼び出されたかを確認できます。AWS では、週に一度のミーティングを実施して、 運用パフォーマンスをレビューし、 学んだ教訓をチーム間で共有しています。 AWS には多数のチームが存在するため、 私たちは The Wheel を作成し、 ワークロードをランダムに選んで確認できるようにしました。運用パフォーマンスのレビューと知識の共有を定期的に行うことで、運用チームのパフォーマンスを向上させることができます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_monitor_aws_resources_review_monitoring.html
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。		-	AWS は、自動モニタリングシステムを活用して、ハイレベルなサービスパフォーマンスと可用性を提供します。内部的、外部的両方の使用において、様々なオンラインツールを用いた積極的モニタリングが可能です。AWS 内のシステムには膨大な装置が備わっており、主要なオペレーションメトリックをモニタリングしています。重要計測値が早期警戒しきい値を超える場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。オンコールスケジュールが採用されているので、担当者が運用上の問題にいつでも対応できます。 AWS は、AWS サービスチームおよびセキュリティチームによって決定されるしきい値アラーム生成メカニズムに基づいて、AWS のモニタリングツールからセキュリティ侵害または潜在的なセキュリティの兆候が示されると、ほぼリアルタイムでアラートします。	

実46	-			2		ログファイルとメトリクスの履歴を収集し、これらを分析して、幅広いトレンドとワークロードの洞察が得られます。Amazon CloudWatch Logs Insights は、 シンプルかつ強力なクエリ言語をサポートし、 ログデータの分析に使用できます。 Amazon CloudWatch Logs ではさらに、シームレスにデータを Amazon S3 に送ってデータを使用したり、または Amazon Athena に送ってデータをクエリしたりできるサブスクリプションもサポートしています。 豊富な種類のフォーマットのクエリがサポートされています。把握 サポートされる SerDes とデータ形式 詳細については、Amazon Athena ユーザーガイドを参照してください。巨大なログファイルセットの分析では、 Amazon EMR クラスターを実行してペタバイト規模の分析を実行できます。 集計、処理、保存、分析を実行できる多数のツールが AWS パートナーやサードパーティによって提供されています。このようなツールには、New Relic、Splunk、Loggly、Logstash、CloudHealth、Nagios などがあります。ただし、システムやアプリケーションログの外で行うデータ生成は各クラウドプロバイダーに固有であり、また多くの場合サービスごとに固有です。モニタリングプロセスで見落とされがちな点は、データ管理です。モニタリングのためのデータ保存要件を決定し、それに応じたライフサイクルポリシーを適用する必要があります。Amazon S3 はS3 バケットレベルのライフサイクル管理をサポートしています。 このライフサイクル管理には、バケット内のパスごとに異なる管理方法を適用できます。ライフサイクルの最終段階では、データを Amazon S3 Glacier に移行して長期保存し、保存期間の終了後には期限切れにすることができます。S3 Intelligent-Tiering ストレージクラスは、パフォーマンスへの影響や運用のオーバーヘッドなしに、データを最も費用対効果の高いアクセス階層に自動的に移動することにより、コストを最適化できるように設計されています。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_monitor_aws_resources_storage_analytics.html
実47	-			3		AWS Cost Explorerで時間単位の粒度を有効にし、 AWS Cost and Usage Report (CUR)を作成します。これらのデータソースは、組織全体のコストと使用量の最も正確なビューを提供します。CUR では、課金されるすべての AWS のサービスについて、日単位または時間単位の使用量の粒度、料金、コスト、使用属性が提供されます。CUR には、タグ付け、場所、リソース属性、アカウント ID など想定可能なすべてのディメンションがあります。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/cost-optimization-pillar/cost_monitor_usage_detailed_source.html Service Quotas は、250 を超える AWS のサービスのクォータを一元的に管理するのに役立つ AWS のサービスです。クォータ値の検索に加えて、Service Quotas コンソールから、または AWS SDK を使用してクォータ増加をリクエスト、追跡することもできます。AWS Trusted Advisor には、あるサービスの一部の要素に関する使用状況とクォータを表示するサービスクォータチェックが用意されています。サービスごとのデフォルトのサービスクォータは、それぞれのサービスの AWS ドキュメントにも記載されています (例えば、Amazon VPC クォータを参照してください)。スロットルされた API のレート制限など、一部のサービス上の制限は、Amazon API Gateway 内で使用量プランを変更することで設定できます。 それぞれのサービス上の構成として設定される一部の制限には、プロビジョンド IOPS、割り当てられた Amazon RDS ストレージ、Amazon EBS ボリューム割り当てなどがあります。Amazon Elastic Compute Cloud には、インスタンス、Amazon Elastic Block Store、および Elastic IP アドレスの制限を管理するのに役立つ独自のサービスの制限ダッシュボードがあります。サービスクォータがアプリケーションのパフォーマンスに影響を及ぼし、ニーズに合わせて調整できないような事例が発生した場合は、AWS Support に連絡し、緩和策の有無についてお問い合わせください。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_manage_service_limits_aware_quotas_and_constraints.html

実47	-			4		多くの AWS サービスは、需要に合わせて自動的にスケールします。Amazon EC2 インスタンスまたは Amazon ECS クラスターを使用している場合、ワークロードの需要に対応する使用状況のメトリクスに基づいて Auto Scaling を実行するように設定できます。Amazon EC2 では、平均 CPU 使用率、ロードバランサーリクエスト数、またはネットワーク帯域幅を使用して、EC2 インスタンスをスケールアウト (またはスケールイン) できます。Amazon ECS では、平均 CPU 使用率、ロードバランサーリクエスト数、およびメモリ使用率を使用して、ECS タスクをスケールアウト (またはスケールイン) できます。AWS で Target Auto Scaling を使用すると、オートスケーラーは家庭用サーモスタットのように機能し、指定したターゲット値 (例えば、CPU 使用率 70%) を維持するためにリソースを追加または削除します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_adapt_to_changes_proactive_adapt_auto.html
実48	-			10		設定を変更し、変更を追跡記録するには、構成管理システムを使用します。これらのシステムは、手動プロセスによって発生するエラーと、変更を導入する労力を減らします。静的な構成管理では、ライフタイムを通じて一貫性を維持することが期待されるリソースの初期化時に値を設定します。このケースの例として、インスタンス上のアプリケーションサーバーまたはウェブサーバー用の構成を設定する場合や、 AWS Management Console 内または AWS CLI を介して AWS サービスの構成を定義する場合が挙げられます。動的な構成管理では、ライフタイムを通じて変化する、または変化することが予測されるリソースの初期化時に値を設定します。例えば、構成変更を介してコードの機能を有効にするように機能トグルを設定したり、インシデント発生時にログの詳細レベルを変更してより多くのデータを取得し、インシデント終了時に詳細レベルを元に戻して不要なログや負荷を減らしたりすることができます。インスタンス、コンテナ、サーバーレス機能、またはデバイスで実行されているアプリケーションで動的な構成を使用している場合、 AWS AppConfig を使用して 環境全体での管理と実装を行うことができます。AWS では、 AWS Config を使用して アカウントおよびリージョン全体の AWS リソース構成を 継続的にモニタリングできます。 そうすることで、構成履歴の追跡、構成変化の他のリソースへの影響、 AWS Config Rules および AWS Config コンフォーマンスパックを使用した期待される、または望まれる設定との比較監査を行えます。AWS では、以下のサービスを使用して、継続的インテグレーションと継続的デプロイ (CI/CD) パイプラインを構築できます。 AWS デベロッパーツール (例: AWS CodeCommit、 AWS CodeBuild、 AWS CodePipeline、 AWS CodeDeploy、および AWS CodeStar)。Change Calendar を用意して、変更の実施によって影響を受ける可能性のある重要なビジネスや運用上の活動やイベントが計画されている時期を追跡します。アクティビティを調整して、これらの計画に関するリスクを管理します。 AWS Systems Manager Change Calendar は、変更に対して時間ブロックがオープンであるかクローズであるか、およびその理由を文書化し、 その情報を他の AWS アカウント と共有します。AWS Systems Manager Automation スクリプトは、カレンダーの変化に沿って実行されるように設定できます。AWS Systems Manager メンテナンスウィンドウは、 AWS SSM Run Command または Automation スクリプト、AWS Lambda 呼び出し、または AWS Step Functions アクティビティの実行を指定した時間にスケジュールできます。これらのアクティビティを評価に含めることができるように、Change Calendar 上で印を付けます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/ops_dev_integ_conf_mgmt_sys.html

実48	-			11		AWS セキュリティブログは、新しい AWS サービスおよび機能、実装ガイド、および一般的なセキュリティガイダンスを取り上げます。「AWS の最新情報」(http://aws.amazon.com/new)は、すべての AWS 機能、サービス、および発表に関する最新情報を確認する優れた方法です。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_securely_operate_implement_services_features.html
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。		-	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。	
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。		-	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。	

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。		-	・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。 ・データセンターの電力システムは、完全に冗長化され、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。AWS は、施設内の重要かつ不可欠な業務に対応するために、電力障害時に運用を維持するための電力供給を可能とするバックアップ電源がデータセンターに備わっていることを保証しています。 ・AWS データセンターは、環境を制御するとともに、サーバーやその他のハードウェアの適切な運用温度を保ち、過熱を防ぎ、サーバー停止の可能性を減らすためのメカニズムを使用しています。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。 ・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 は、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。	
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。		-	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。	

		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			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定義の論理統制と物理統制の定義は、SOC 1 Type IIレポートに文書化されています。また、このレポートは、この監査チームとコンプライアンスチームのレビューに使用できます。また、AWS ISO 27001およびその他の認定も、監査人のレビュー用に使用できます。物理的セキュリティ統制には、フェンス、壁、保安要員、監視カメラ、侵入検知システムその他の電子的手段による周辺統制が含まれますが、これに限定されるものではありません。物理的アクセスは、建物の周辺および入り口において、監視カメラや侵入検知システムなどの電子的手段を用いる専門の保安要員その他の手段により、厳重に管理されています。権限を付与されたスタッフが2要素認証を最低2回用いて、データセンターのフロアにアクセスします。サーバー設置箇所への物理アクセスポイントは、AWSデータセンター物理セキュリティポリシーの規定により、閉回路テレビ(CCTV)カメラで録画されています。録画は90日間保存されます。ただし、法的または契約義務により30日間に制限される場合もあります。AWSは、このような特権を必要とする正規の業務を有する承認済みの従業員や契約社員に対して、データセンターへの物理的なアクセス権や情報を提供しています。すべての訪問者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが付き添いを行います。物理的なアクセス、データセンターへのアクセスの承認、その他の関連統制については、SOC 1 Type IIレポートを参照してください。 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。	
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。			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定義の論理統制と物理統制の定義は、SOC 1 Type IIレポートに文書化されています。また、このレポートは、この監査チームとコンプライアンスチームのレビューに使用できます。また、AWS ISO 27001およびその他の認定も、監査人のレビュー用に使用できます。物理的セキュリティ統制には、フェンス、壁、保安要員、監視カメラ、侵入検知システムその他の電子的手段による周辺統制が含まれますが、これに限定されるものではありません。物理的アクセスは、建物の周辺および入り口において、監視カメラや侵入検知システムなどの電子的手段を用いる専門の保安要員その他の手段により、厳重に管理されています。権限を付与されたスタッフが2要素認証を最低2回用いて、データセンターのフロアにアクセスします。サーバー設置箇所への物理アクセスポイントは、AWSデータセンター物理セキュリティポリシーの規定により、閉回路テレビ(CCTV)カメラで録画されています。録画は90日間保存されます。ただし、法的または契約義務により30日間に制限される場合もあります。AWSは、このような特権を必要とする正規の業務を有する承認済みの従業員や契約社員に対して、データセンターへの物理的なアクセス権や情報を提供しています。すべての訪問者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが付き添いを行います。物理的なアクセス、データセンターへのアクセスの承認、その他の関連統制については、SOC 1 Type IIレポートを参照してください。 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。	

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。		-	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定義の論理統制と物理統制の定義は、SOC 1 Type IIレポートに文書化されています。また、このレポートは、この監査チームとコンプライアンスチームのレビューに使用できます。また、AWS ISO 27001およびその他の認定も、監査人のレビュー用に使用できます。物理的セキュリティ統制には、フェンス、壁、保安要員、監視カメラ、侵入検知システムその他の電子的手段による周辺統制が含まれますが、これに限定されるものではありません。物理的アクセスは、建物の周辺および入り口において、監視カメラや侵入検知システムなどの電子的手段を用いる専門の保安要員その他の手段により、厳重に管理されています。権限を付与されたスタッフが2要素認証を最低2回用いて、データセンターのフロアにアクセスします。サーバー設置箇所への物理アクセスポイントは、AWSデータセンター物理セキュリティポリシーの規定により、閉回路テレビ(CCTV)カメラで録画されています。録画は90日間保存されます。ただし、法的または契約義務により30日間に制限される場合もあります。AWSは、このような特権を必要とする正規の業務を有する承認済みの従業員や契約社員に対して、データセンターへの物理的なアクセス権や情報を提供しています。すべての訪問者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが付き添いを行います。物理的なアクセス、データセンターへのアクセスの承認、その他の関連統制については、SOC 1 Type IIレポートを参照してください。 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。	

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。		-	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定義の論理統制と物理統制の定義は、SOC 1 Type IIレポートに文書化されています。また、このレポートは、この監査チームとコンプライアンスチームのレビューに使用できます。また、AWS ISO 27001およびその他の認定も、監査人のレビュー用に使用できます。物理的セキュリティ統制には、フェンス、壁、保安要員、監視カメラ、侵入検知システムその他の電子的手段による周辺統制が含まれますが、これに限定されるものではありません。物理的アクセスは、建物の周辺および入り口において、監視カメラや侵入検知システムなどの電子的手段を用いる専門の保安要員その他の手段により、厳重に管理されています。権限を付与されたスタッフが2要素認証を最低2回用いて、データセンターのフロアにアクセスします。サーバー設置箇所への物理アクセスポイントは、AWSデータセンター物理セキュリティポリシーの規定により、閉回路テレビ(CCTV)カメラで録画されています。録画は90日間保存されます。ただし、法的または契約義務により30日間に制限される場合もあります。AWSは、このような特権を必要とする正規の業務を有する承認済みの従業員や契約社員に対して、データセンターへの物理的なアクセス権や情報を提供しています。すべての訪問者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが付き添いを行います。物理的なアクセス、データセンターへのアクセスの承認、その他の関連統制については、SOC 1 Type IIレポートを参照してください。 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。	

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。		-	設備のメンテナンス 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。 環境管理 AWS は、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。 CCTV サーバールームに物理的にアクセスできる場所は、閉回路テレビカメラ（CCTV）によって録画されています。画像イメージは、法律およびコンプライアンスに関する要件に従って保持されます。 データセンターのエントリポイント 物理的アクセスは、建物の入り口において、サーベイランスシステム、侵入検知システム、その他の電子的システムを用いて、専門の保安要員によって厳重に管理されています。権限を付与されたスタッフは、多要素認証のメカニズムを利用してデータセンターにアクセスします。サーバールームへの入り口は、ドアがこじ開けられた場合や開け放したままの場合にデバイスでアラームを鳴らし、インシデント対応を開始するように設置された装置で保護されています。 侵入検知 データレイヤー内の場所に電子的手段による進入検出システムが設置され、セキュリティインシデントのモニタリング、検出、および適切な人員への自動的なアラート通知が行われます。サーバールームの入り口および出口は、入場または退場が許可される際に多要素認証を各個人に求める装置で保護されています。これらのデバイスは、許可なくドアがこじ開けられた場合や開け放したままの場合にはアラームを鳴らします。また、ドアのアラームデバイスは、多要素認証を提供せずにデータレイヤーに入場または退場した事例を検出するよう設定されてもいます。アラームは即時のログ記録、分析、および応答のため、24 時間 365 日にわたり AWS セキュリティオペレーションセンターに即時に送信されます。	
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。		-	AWS の従業員は、疑わしいセキュリティインシデントの見分け方と報告先についてトレーニングを受けています。条件に該当する場合は、インシデントが関係機関等に報告されます。AWS は、AWS サービスに影響を及ぼすセキュリティイベントおよびプライバシーイベントをお客様にお知らせする AWS Security Bulletinウェブページを運営しています。Security Bulletin の RSS フィードに登録すると、Security Bulletin ウェブページでの最新のセキュリティ通知を常に把握できます。お客様サポートチームは、可用性に広範な影響を及ぼしている問題についてお客様にアラートを出すサービス状態ダッシュボードのウェブページを運営しています。	

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。		-	AWS における復元力の高いインフラストラクチャ、信頼性の高い自動化、統制の取れたプロセス、優れた人員を活用すると、お客様の側で処理中断が生じた場合でも、それを最小限に抑え、該当イベントから迅速に復旧できます。AWS の事業継続計画には、AWS のインフラストラクチャの復旧と再構成を目的として開発された、以下の3フェーズのアプローチが詳しく記載されています。 •アクティベーションと通知のフェーズ •復旧のフェーズ •再構成のフェーズ このアプローチによって、AWS がシステムの復旧と再構成に関する取り組みを体系的な順序で実施することが保証され、取り組みの有効性が最大限に高まり、エラーや作業漏れに起因するシステムの稼働停止時間が最小限に抑えられます。AWS は、すべてのリージョンにわたるユビキタスなセキュリティ制御の環境を維持管理しています。各データセンターは、物理、環境、セキュリティに関する基準に沿ってアクティブ - アクティブ構成として構築されており、n+1 の冗長モデルを採用することによって、コンポーネントに障害が発生した際のシステム可用性を確保しています。コンポーネント(N 個) に対して、少なくとも1 つの独立したバックアップコンポーネント(+1) が配置されており、このバックアップコンポーネントは、運用環境に含まれている他のすべてのコンポーネントが順調に機能している場合もアクティブになります。単一障害点を解消することを目的として、ネットワークとデータセンターの導入を含め、このモデルがAWS 全体で適用されています。すべてのデータセンターがオンラインとなってトラフィックを提供しています。「コールド」状態のデータセンターは存在しません。障害が発生した際も、残りのサイトにトラフィックの負荷を分散できる十分な処理能力が確保されています。 AWS は、インシデント対応に関して、文書化された正式な方針およびプログラムを導入しています。この方針では、目的、範囲、役割、責任、経営者のコミットメントが取り上げられています。AWS は、以下の3 つのフェーズに分かれるインシデント管理アプローチを採用しています。1.アクティベーションと通知のフェーズ2.復旧のフェーズ3.再構成のフェーズAWS のインシデント管理計画から確実な効果が得られるように、AWS はインシデント対応のテストを実施します。このテストでは、その時点の未知の不具合と障害モードについて広い範囲を検出対象としてカバーします。さらに、Amazon のセキュリティチームおよびサービスチームは、お客様への潜在的な影響の有無についてシステムをテストし、検知と分析、封じ込め、除去、復旧、インシデント処理後のアクティビティなど、インシデントの処理に携わる要員を準備することが可能になります。インシデント対応計画と併せて、インシデント対応テスト計画を年1 回作成します。AWS のインシデント管理の計画を作成し、テストを実施し、テスト結果は、第三者の監査人による審査を受けます	

実71	-			5		回避すべきパターンは、まれにしか実行されない復旧経路を作ることです。たとえば、読み取り専用のクエリに使用されるセカンダリデータストアがあるとします。データストアの書き込み時にプライマリデータストアで障害が発生した場合、セカンダリデータストアにフェイルオーバーします。もしこのフェイルオーバーを頻繁にテストしない場合、セカンダリデータストアの機能に関する前提が正しくない可能性があります。セカンダリデータストアの容量は、最後にテストしたときには十分だったかもしれませんが、このシナリオでは負荷に耐えられなくなる可能性があります。エラー復旧がうまくいくのは頻繁にテストする経路のみであることは、これまでの経験からも明らかです。少数の復旧経路を用意することがベストであるのはそのためです。復旧パターンを確立して定期的にテストできます。復旧経路が複雑な場合や重大な場合に復旧経路が正常に機能するという確信を持つには、本番環境でその障害を定期的に実行する必要があります。前述の例では、その必要性に関係なく、スタンバイへのフェイルオーバーを定期的に行う必要があります。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_planning_for_recovery_dr_tested.html AWS Resilience Hub でワークロードの RTO や RPO を含むレジリエンスポリシーを定義することで、構成されるインフラストラクチャやアプリケーション設定などを評価することができます。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/reliability.md
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。			-	AWS は、インシデント対応に関して、文書化された正式な方針およびプログラムを導入しています。この方針では、目的、範囲、役割、責任、経営者のコミットメントが取り上げられています。AWS は、以下の3 つのフェーズに分かれるインシデント管理アプローチを採用しています。1.アクティベーションと通知のフェーズ2.復旧のフェーズ3.再構成のフェーズAWS のインシデント管理計画から確実な効果が得られるように、AWS はインシデント対応のテストを実施します。このテストでは、その時点の未知の不具合と障害モードについて広い範囲を検出対象としてカバーします。さらに、Amazon のセキュリティチームおよびサービスチームは、お客様への潜在的な影響の有無についてシステムをテストし、検知と分析、封じ込め、除去、復旧、インシデント処理後のアクティビティなど、インシデントの処理に携わる要員を準備することが可能になります。インシデント対応計画と併せて、インシデント対応テスト計画を年1 回作成します。AWS のインシデント管理の計画を作成し、テストを実施し、テスト結果は、第三者の監査人による審査を受けます。	
実72	-			8		AWS Health Dashboardでは、AWS サービスの可用性と運用状況を 1 か所で確認できます。AWS サービスの全体的なステータスを表示できます。また、サインインすると、特定の AWS アカウントまたは組織に関するパーソナライズされたコミュニケーションを表示できます。アカウントビューでは、リソースの問題、今後の変更、重要な通知をより詳細に把握できます。 https://docs.aws.amazon.com/ja_jp/health/latest/ug/what-is-aws-health.html

実72	-			9		AWS Health Dashboard のサービス履歴では、過去12カ月間のAWSサービスの中断が表示されます。 https://health.aws.amazon.com/health/status
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。		-	[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] AWSのビジネス継続性ポリシーおよび計画は、ISO 27001基準に合わせて開発され、テストされています。AWSとビジネス継続性の詳細については、ISO 27001基準の付録A、ドメイン17を参照してください。 [可用性] AWS データセンターは、世界のさまざまなリージョンにクラスター化されて構築されています。すべてのデータセンターはオンラインで顧客にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、影響を受けたエリアから顧客データが移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。AWS は、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。各アベイラビリティーゾーンは、独立した障害ゾーンとして設計されています。つまり、アベイラビリティーゾーンは、一般的な都市地域内で物理的に分離されており、洪水の影響が及ばないような場所にあります(洪水地域の分類はリージョンによって異なります)。個別の無停電電源装置(UPS) やオンサイトのバックアップ生成施設に加え、シングルポイントの障害の可能性を減らすために、別々の電力供給施設から異なる配管網を経由して、個別に電力供給を行っています。これらはすべて、冗長的に、複数のTier-1 プロバイダーに接続されています。顧客は AWS の使用量を計画しながら、複数のリージョンやアベイラビリティーゾーンを利用する必要があります。複数のアベイラビリティーゾーンにアプリケーションを配信することによって、自然災害やシステム障害など、ほとんどの障害モードに対して、その可用性を保つことができます。	

		[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。			[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73	-			8		単一の AWS リージョン 内の複数のアベイラビリティゾーン (AZ) にまたがる DR 戦略は、火災、洪水、大規模な停電などの災害イベントに対して影響を緩和できます。ワークロードを特定の AWS リージョン で実行できなくなるような、可能性の低いイベントに対する保護を実装する必要がある場合には、複数のリージョンを使用する DR 戦略を使用できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_planning_for_recovery_disaster_recovery.html
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。		-	AWS データセンターは、世界のさまざまなリージョンにクラスター化されて構築されています。すべてのデータセンターはオンラインで顧客にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、影響を受けたエリアから顧客データが移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。AWS は、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。各アベイラビリティーゾーンは、独立した障害ゾーンとして設計されています。つまり、アベイラビリティーゾーンは、一般的な都市地域内で物理的に分離されており、洪水の影響が及ばないような場所にあります(洪水地域の分類はリージョンによって異なります)。個別の無停電電源装置(UPS) やオンサイトのバックアップ生成施設に加え、シングルポイントの障害の可能性を減らすために、別々の電力供給施設から異なる配管網を経由して、個別に電力供給を行っています。これらはすべて、冗長的に、複数のTier-1 プロバイダーに接続されています。顧客は AWS の使用量を計画しながら、複数のリージョンやアベイラビリティーゾーンを利用する必要があります。複数のアベイラビリティーゾーンにアプリケーションを配信することによって、自然災害やシステム障害など、ほとんどの障害モードに対して、その可用性を保つことができます。	

実74	-			4		単一の AWS リージョン 内の複数のアベイラビリティゾーン (AZ) にまたがる DR 戦略は、火災、洪水、大規模な停電などの災害イベントに対して影響を緩和できます。ワークロードを特定の AWS リージョン で実行できなくなるような、可能性の低いイベントに対する保護を実装する必要がある場合には、複数のリージョンを使用する DR 戦略を使用できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_planning_for_recovery_disaster_recovery.html AWSリージョンやデータセンターの設計を踏まえ、日本における地震災害において、どのようにAWSが高い耐障害性を確保しているか、また、マルチリージョンの活用により、お客様がどのように高いレジリエンスを確保できるかを解説したホワイトペーパーを、AWS Artifactおいて公開しています。 https://aws.amazon.com/jp/blogs/news/resiliency-in-japan/
実76	-			3		AWS では、社内のレポート構造を流用せずに、個別アカウントごとにワークロードを整理し、機能、コンプライアンス要件、共通のコントロールセットに基づいてアカウントをグループ化することを推奨しています。AWS では、アカウントが強固な境界となります。たとえば、開発およびテストのワークロードと本番ワークロードを切り離すために、アカウントレベルの分離を強く推奨しています。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/aws-account-management-and-separation.html
実82	-			3		AWS環境における安全なデータ廃棄の方法の例は、以下の記事をご参照ください。 クラウドにおける安全なデータの廃棄 https://aws.amazon.com/jp/blogs/news/data_disposal/ クラウドにおける安全なデータの廃棄（実践編） https://aws.amazon.com/jp/blogs/news/delstoragedatapractice/

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。		-	AWS における復元力の高いインフラストラクチャ、信頼性の高い自動化、統制の取れたプロセス、優れた人員を活用すると、お客様の側で処理中断が生じた場合でも、それを最小限に抑え、該当イベントから迅速に復旧できます。AWS の事業継続計画には、AWS のインフラストラクチャの復旧と再構成を目的として開発された、以下の3フェーズのアプローチが詳しく記載されています。 •アクティベーションと通知のフェーズ •復旧のフェーズ •再構成のフェーズ このアプローチによって、AWS がシステムの復旧と再構成に関する取り組みを体系的な順序で実施することが保証され、取り組みの有効性が最大限に高まり、エラーや作業漏れに起因するシステムの稼働停止時間が最小限に抑えられます。AWS は、すべてのリージョンにわたるユビキタスなセキュリティ制御の環境を維持管理しています。各データセンターは、物理、環境、セキュリティに関する基準に沿ってアクティブ - アクティブ構成として構築されており、n+1 の冗長モデルを採用することによって、コンポーネントに障害が発生した際のシステム可用性を確保しています。コンポーネント(N 個) に対して、少なくとも1 つの独立したバックアップコンポーネント(+1) が配置されており、このバックアップコンポーネントは、運用環境に含まれている他のすべてのコンポーネントが順調に機能している場合もアクティブになります。単一障害点を解消することを目的として、ネットワークとデータセンターの導入を含め、このモデルがAWS 全体で適用されています。すべてのデータセンターがオンラインとなってトラフィックを提供しています。「コールド」状態のデータセンターは存在しません。障害が発生した際も、残りのサイトにトラフィックの負荷を分散できる十分な処理能力が確保されています。	
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。		-	AWS における復元力の高いインフラストラクチャ、信頼性の高い自動化、統制の取れたプロセス、優れた人員を活用すると、お客様の側で処理中断が生じた場合でも、それを最小限に抑え、該当イベントから迅速に復旧できます。AWS の事業継続計画には、AWS のインフラストラクチャの復旧と再構成を目的として開発された、以下の3フェーズのアプローチが詳しく記載されています。 •アクティベーションと通知のフェーズ •復旧のフェーズ •再構成のフェーズ このアプローチによって、AWS がシステムの復旧と再構成に関する取り組みを体系的な順序で実施することが保証され、取り組みの有効性が最大限に高まり、エラーや作業漏れに起因するシステムの稼働停止時間が最小限に抑えられます。AWS は、すべてのリージョンにわたるユビキタスなセキュリティ制御の環境を維持管理しています。各データセンターは、物理、環境、セキュリティに関する基準に沿ってアクティブ - アクティブ構成として構築されており、n+1 の冗長モデルを採用することによって、コンポーネントに障害が発生した際のシステム可用性を確保しています。コンポーネント(N 個) に対して、少なくとも1 つの独立したバックアップコンポーネント(+1) が配置されており、このバックアップコンポーネントは、運用環境に含まれている他のすべてのコンポーネントが順調に機能している場合もアクティブになります。単一障害点を解消することを目的として、ネットワークとデータセンターの導入を含め、このモデルがAWS 全体で適用されています。すべてのデータセンターがオンラインとなってトラフィックを提供しています。「コールド」状態のデータセンターは存在しません。障害が発生した際も、残りのサイトにトラフィックの負荷を分散できる十分な処理能力が確保されています。	

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。		-	AWS における復元力の高いインフラストラクチャ、信頼性の高い自動化、統制の取れたプロセス、優れた人員を活用すると、お客様の側で処理中断が生じた場合でも、それを最小限に抑え、該当イベントから迅速に復旧できます。AWS の事業継続計画には、AWS のインフラストラクチャの復旧と再構成を目的として開発された、以下の3フェーズのアプローチが詳しく記載されています。 •アクティベーションと通知のフェーズ •復旧のフェーズ •再構成のフェーズ このアプローチによって、AWS がシステムの復旧と再構成に関する取り組みを体系的な順序で実施することが保証され、取り組みの有効性が最大限に高まり、エラーや作業漏れに起因するシステムの稼働停止時間が最小限に抑えられます。AWS は、すべてのリージョンにわたるユビキタスなセキュリティ制御の環境を維持管理しています。各データセンターは、物理、環境、セキュリティに関する基準に沿ってアクティブ - アクティブ構成として構築されており、n+1 の冗長モデルを採用することによって、コンポーネントに障害が発生した際のシステム可用性を確保しています。コンポーネント(N 個) に対して、少なくとも1 つの独立したバックアップコンポーネント(+1) が配置されており、このバックアップコンポーネントは、運用環境に含まれている他のすべてのコンポーネントが順調に機能している場合もアクティブになります。単一障害点を解消することを目的として、ネットワークとデータセンターの導入を含め、このモデルがAWS 全体で適用されています。すべてのデータセンターがオンラインとなってトラフィックを提供しています。「コールド」状態のデータセンターは存在しません。障害が発生した際も、残りのサイトにトラフィックの負荷を分散できる十分な処理能力が確保されています。	
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。		-	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 リージョン内のすべての AZ は、AZ 間に高スループットかつ低レイテンシーのネットワーキングを提供する、完全に冗長性を持つ専用メトロファイバー上に構築された、高帯域幅、低レイテンシーのネットワーキングで相互接続されています。	

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。		-	AWS における復元力の高いインフラストラクチャ、信頼性の高い自動化、統制の取れたプロセス、優れた人員を活用すると、お客様の側で処理中断が生じた場合でも、それを最小限に抑え、該当イベントから迅速に復旧できます。AWS の事業継続計画には、AWS のインフラストラクチャの復旧と再構成を目的として開発された、以下の3フェーズのアプローチが詳しく記載されています。 •アクティベーションと通知のフェーズ •復旧のフェーズ •再構成のフェーズ このアプローチによって、AWS がシステムの復旧と再構成に関する取り組みを体系的な順序で実施することが保証され、取り組みの有効性が最大限に高まり、エラーや作業漏れに起因するシステムの稼働停止時間が最小限に抑えられます。 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。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。	
実99	-			3		ランブックは、特定の成果を達成するために文書化されたプロセスです。ランブックは一連のステップから成り、それをたどることでプロセスを完了できます。ランブックは、飛行機の黎明期から運用に使用されてきました。クラウド運用では、ランブックを使用してリスクを削減し、望ましい成果を達成します。端的に言うと、ランブックはタスクを完了するためのチェックリストです。 ランブックは、組織の成熟度に応じて、いくつかの形態をとります。少なくとも、ステップバイステップのテキスト文書で構成されている必要があります。期待される成果が明確に示されている必要があります。必要な特殊なアクセス許可やツールを明確に文書化します。問題発生時にエラー処理とエスカレーションに関する詳細なガイダンスを提供します。ランブックの所有者をリストアップし、一元的な場所で公開します。ランブックが文書化されたら、チームの別のメンバーに使用してもらって検証します。プロセスの進化につれて、変更管理プロセスに従ってランブックを更新します。

						組織が成熟するにつれて、テキストのランブックは自動化されるはずです。例えば、 AWS Systems Manager オートメーションなどのサービスを使用すると、フラットなテキストを、ワークロードに対して実行可能なオートメーションに変換できます。これらのオートメーションはイベントに反応して実行でき、ワークロードを保守する運用上の負担が軽減されます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/ops_ready_to_support_use_runbooks.html 自動スケーリングまたは自動復旧を使用できない場合、または自動復旧が失敗した場合は、AWS Step Functions と AWS Lambda を使用して自動復旧を実装します。自動スケーリングを使用できず、さらに、自動復旧が使用できないか、自動復旧が失敗した場合は、AWS Step Functions と AWS Lambda を使用して修復を自動化できます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_withstand_component_failures_auto_healing_system.html
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。		-	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。	

実100	-			4		AWS には、脆弱性管理プログラムに役立つ様々なサービスがあります。Amazon Inspector は、ソフトウェアの問題と意図しないネットワークアクセスを検出するために、継続的に AWS ワークロードをスキャンします。AWS Systems Manager Patch Manager を使うと、Amazon EC2 インスタンス全体のパッチ適用を管理できます。Amazon Inspector と Systems Manager は、AWS Security Hub で表示できます。これは、AWS セキュリティチェックを自動化して、セキュリティアラートを一元化するのに役立つクラウドセキュリティ体制管理サービスです。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_compute_vulnerability_management.html AWS Config は、設定が誤っているリソースを報告し、AWS Config ポリシーチェックを通して、パブリックアクセスが設定されたリソースを検出できます。AWS Control TowerやAWS Security Hubなどのサービスでは、AWS Organizations 全体でチェックとガードレールのデプロイが簡素化され、公開されたリソースを特定および修復します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_permissions_analyze_cross_account.html
実101	-			3		需要に合わせてリソースをプロアクティブにスケールし、可用性への影響を回避します。 多くの AWS サービスは、需要に合わせて自動的にスケールします。Amazon EC2 インスタンスまたは Amazon ECS クラスターを使用している場合、ワークロードの需要に対応する使用状況のメトリクスに基づいて Auto Scaling を実行するように設定できます。Amazon EC2 では、平均 CPU 使用率、ロードバランサーリクエスト数、またはネットワーク帯域幅を使用して、EC2 インスタンスをスケールアウト (またはスケールイン) できます。Amazon ECS では、平均 CPU 使用率、ロードバランサーリクエスト数、およびメモリ使用率を使用して、ECS タスクをスケールアウト (またはスケールイン) できます。AWS で Target Auto Scaling を使用すると、オートスケーラーは家庭用サーモスタットのように機能し、指定したターゲット値 (例えば、CPU 使用率 70%) を維持するためにリソースを追加または削除します。 AWS Auto Scaling はまた、 Predictive Auto Scaling も実行できます。これは、機械学習を使用して各リソースの過去のワークロードを分析し、次の 2 日間の負荷を定期的に予測します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/design-your-workload-to-adapt-to-changes-in-demand.html

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。		-	AWS は、自動モニタリングシステムを活用して、ハイレベルなサービスパフォーマンスと可用性を提供します。内部的、外部的両方の使用において、様々なオンラインツールを用いた積極的モニタリングが可能です。AWS 内のシステムには膨大な装置が備わっており、主要なオペレーションメトリックをモニタリングしています。重要計測値が早期警戒しきい値を超える場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。オンコールスケジュールが採用されているので、担当者が運用上の問題にいつでも対応できます。	
実102	-			3		ワークロードを設計する際には、可観測性と問題調査への対応においてすべてのコンポーネントにわたって内部状態 (メトリクス、ログ、イベント、トレースなど) を理解するために必要な情報が送出されるようにします。ワークロードの稼働状態を監視し、結果にリスクがあった場合にそれを特定し、効果的な対応を可能にするために必要なテレメトリの開発を繰り返します。AWS ではアプリケーションとワークロードコンポーネントからログ、メトリクス、イベントを送出して収集し、内部的な状況と稼働状態を把握できます。分散トレースを統合して、ワークロードを通過するリクエストを追跡できます。このデータを使用して、アプリケーションと基盤となるコンポーネントがどのように相互作用するかを理解し、問題とパフォーマンスを分析します。ワークロードを計測する際は、フィルターを使用して時間の経過とともに最も有用な情報を選択できるので、状況認識を可能にする幅広い情報 (状態の変化、ユーザーのアクティビティ、権限アクセス、使用量のカウンターなど) を取得します。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/design-telemetry.htm IAWS は、Service Health Dashboard でサービスの可用性に関する最新情報を公開しています。いつでも確認して最新のステータス情報を入手したり、RSSフィードを購読して個々のサービスの中断の通知を受けたりすることができます。AWS のいずれかのサービスでリアルタイムの運用上の問題が発生し、それが Service Health Dashboard に表示されない場合は、サポートリクエストを作成できます。AWS Health Dashboard には、アカウントに影響する可能性がある AWS Health イベントの情報が表示されます。情報は 2 つの方法で表示されます。ダッシュボードには、最近のイベントおよび予定されているイベントがカテゴリ別に分類されて表示されます。詳細なイベントログには、過去 90 日間のすべてのイベントが表示されます。 https://docs.aws.amazon.com/ja_jp/whitepapers/latest/disaster-recovery-workloads-on-aws/detection.html

実102	-			2	AWS は、AWS クラウド で提供されるすべてのサービスを実行するインフラストラクチャの回復性について責任を負います。このインフラストラクチャは、AWS クラウド サービスを実行するハードウェア、ソフトウェア、ネットワーク、設備で構成されます。AWS は、このような AWS クラウド サービスを利用可能にするうえで商業的に合理的な取り組みを行い、サービスの可用性が AWS サービスレベルアグリーメント (SLA) を満たすか、それ以上を提供することを確認します。AWS グローバルクラウドインフラストラクチャは、お客様が回復力の高いワークロードアーキテクチャを構築できるように設計されています。各 AWS リージョン は完全に分離されており、物理的に分離されたインフラストラクチャのパーティションである複数のアベイラビリティーゾーンで構成されています。アベイラビリティーゾーンは、ワークロードの回復力に影響を及ぼす可能性のある障害を分離し、リージョン内のその他のゾーンへの影響を回避します。ただし同時に、AWS リージョン 内のすべてのゾーンは、高帯域幅、低レイテンシーのネットワークで相互接続されています。ゾーン間をつなぐのは、高スループット、低レイテンシーのネットワークを提供する、完全な冗長性を備えた専用メトロファイバーです。ゾーン間のすべてのトラフィックは暗号化されています。ゾーン間の同期レプリケーションを実行するうえで十分なネットワークパフォーマンスが提供されます。アプリケーションを AZ 間でパーティショニングすると、企業は、停電、落雷、竜巻、台風などの問題から、よりよく隔離され保護されます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/shared-responsibility-model-for-resiliency.html	お客様の責任は、選択した AWS クラウド サービスにより異なります。選択したサービスにより、お客様が回復性についての責任の一環として実行する必要がある設定作業の量が決まります。例えば、Amazon Elastic Compute Cloud (Amazon EC2) のようなサービスでは、お客様は必要となる回復性の設定と管理をすべて実行する必要があります。Amazon EC2 インスタンスをデプロイするお客様の場合は、Amazon EC2 インスタンスを複数のロケーション (AWS アベイラビリティーゾーンなど) にデプロイして、Auto Scaling などのサービスを使用して、自己修復を実装し、インスタンスにインストールしたアプリケーションに対して回復力のあるワークロードアーキテクチャのベストプラクティスを使用する責任があります。Amazon S3 と Amazon DynamoDB などのマネージドサービスの場合は、インフラストラクチャレイヤー、オペレーティングシステム、プラットフォームの運用を AWS が行い、お客様はエンドポイントにアクセスしてデータを保存、取得します。お客様は、バックアップ、バージョニング、レプリケーション戦略など、データの回復力を管理する責任があります。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/shared-responsibility-model-for-resiliency.html リソース障害の発生時に、正常なリソースが引き続きリクエストに対応できるようにします。ロケーション障害 (アベイラビリティゾーンや AWS リージョン など) に対しては、障害のないロケーションの正常なリソースにフェイルオーバーするシステムを用意します。Elastic Load Balancing や AWS Auto Scaling などの AWS のサービスは、複数のリソースおよびアベイラビリティゾーンへの負荷分散に役立ちます。そのため、個々のリソース (EC2 インスタンスなど) の障害や、アベイラビリティゾーンの障害を、残りの正常なリソースにトラフィックをシフトすることによって緩和できます。 マルチリージョンのワークロードの場合、状況はさらに複雑です。例えば、クロスリージョンリードレプリカを使用すると、データを複数の AWS リージョン にデプロイできますが、障害が発生した場合は、リードレプリカをプライマリに昇格させ、そこにトラフィックを向かわせる必要があります。Amazon Route 53 と AWS Global Accelerator は、AWS リージョン 間のトラフィックのルーティングを容易にします。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/rel_withstand_component_failures_failover2good.html
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。		-	AWS は、自動モニタリングシステムを活用して、ハイレベルなサービスパフォーマンスと可用性を提供します。内部的、外部的両方の使用において、様々なオンラインツールを用いた積極的モニタリングが可能です。AWS 内のシステムには膨大な装置が備わっており、主要なオペレーションメトリックをモニタリングしています。重要計測値が早期警戒しきい値を超える場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。オンコールスケジュールが採用されているので、担当者が運用上の問題にいつでも対応できます。	