

「AWS FISC安全対策基準対応リファレンス」参考文書

「金融機関向け AWS FISC安全対策基準対応リファレンス」（2023年7月公開）対応

第2版 2024年 8月

初版 2022年 2月

作成：株式会社NTTデータ
SCSK株式会社
TIS株式会社
シンプレクス株式会社
株式会社電通総研
トレンドマイクロ株式会社
日本電気株式会社
株式会社野村総合研究所
株式会社日立製作所
富士通株式会社
(五十音順)

【はじめに】

本書は2023年7月にAWSがリリースした「AWS FISC安全対策基準対応リファレンス」に対する参考文書となっています。「AWS FISC安全対策基準対応リファレンス」におけるAWSの対応状況およびお客様が統制すべき内容について、「FISC対応APNコンソーシアム」を構成するベンダーの視点から参考情報を付加しています。

【対象範囲】

AWSが提供する機能および情報等を利用してシステムを実装もしくはサービスの管理をすることを前提としています。AWS環境(AWSのデータセンターを含む)以外の物理環境(金融機関等のコンピューターセンター・共同センター、本部・営業店等)や金融機関等のオンプレミス環境(インターネット回線、外部接続ルーター、業務端末等)、「AWS FISC安全対策基準対応リファレンス」で取り扱われていないFISC安全対策基準の基準は対象外となります。

【本書の見方】

本書にて付加した参考情報は、「参考情報」列にまとめています。「AWS FISC安全対策基準対応リファレンス」からの引用箇所の見方については、「AWS FISC安全対策基準対応リファレンス」に準じます。

[概要]

FISC安全対策基準に対するAWSの対応状況およびAWSの対応状況を踏まえた金融機関等で実施すべき統制の概要について記載しています。

[対処例]

AWSの対応状況について、より具体的な内容を記載しています。

[対策例]

金融機関等で実施すべき統制について、より具体的な内容を記載しています。

[関連する認証]

AWSの対応状況について、第三者保証による報告書または第三者認証に関する情報を通じて確認することが望ましい場合に、関連する報告書または認証の項目番号を記載しています。

[参考文献、参照URL]

参考情報の付加にあたって参照した文献またはwebページのURLについて記載しています。

【利用規約】

免責事項等を含む本書の利用規約については、別添の「利用規約」に準じます。

【改版履歴】

[初版] 2022年2月リリース

[第2版] 2024年8月リリース

「金融機関向け AWS FISC安全対策基準対応リファレンス」（2023年7月公開）に対応して、以下の基準小項目について改訂。

○実務基準

実1、実3、実4、実5、実7、実8、実9、実10、実13、実14、実15、実16、実19、実20、実21、実22
実25、実27、実30、実31、実32、実34、実37、実38、実39、実42、実43、実46、実47、実48、実71
実72、実73、実74、実76、実82、実83、実87、実99、実100、実102、実103、実103-1、

○統制基準

統20 3-(1)、3-(3)、 統22 3、4、 統23 1,2、3

【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

「AWS FISCC安全対策基準対応リファレンス」からの引用					参考情報	補足情報
標準番号	役割	対応の主体		AWSの対応状況		
		AWS	お客様		お客様が統制すべき内容	
-	-	-	-	統制基準はお客様がITガバナンスやITマネジメントを行う上で必要となる組織の内部に関する統制項目（統1～統19）とお客様が外部委託先等、外部の組織に関する統制項目（統20～26）により構成されます。統制基準についてはAWSが対応の主体となる項目はありませんが、お客様がAWSを外部の組織（外部委託先）として評価をされる際に参考となる情報を記載しております。	-	-
				セキュリティとコンプライアンスはAWSとお客様の間で共有される責任です。この共有モデルは、AWSがホストオペレーティングシステムと仮想化レイヤーから、サービスが運用されている施設の物理的なセキュリティに至るまでの要素をAWSが運用、管理、および制御することから、お客様の運用上の負担を軽減するために役立ちます。お客様には、ゲストオペレーティングシステム（OS）とセキュリティパッチを含む、その他の関連アプリケーションソフトウェア、およびAWSが提供するセキュリティグループファイアウォールの設定に対する責任と管理を担っていただきます。使用するサービス、それらのサービスのIT環境への統合、および適用される法律と規制によって責任が異なるため、お客様は選択したサービスを慎重に検討する必要があります。また、この責任共有モデルの性質によって柔軟性が得られ、お客様がデプロイを統制できます。		
				責任共有モデルの詳細については以下のURLを参照ください。 https://aws.amazon.com/ja/compliance/shared-responsibility-model/		
統1		-	○	-	-	-
統1	参考	-	○	・契約時に考慮するべき事項の例としてご参照ください。 AWSの法務関連の情報は以下のサイトをご参照ください。 https://aws.amazon.com/jp/legal/ また、契約、その他法務関連のお問い合わせについては担当営業までご連絡ください。 - AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです - AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます - AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます - AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです ・AWSのカスタマーアグリーメントにおいて、クラウドサービスの販売者がアマゾン ウェブ サービス ジャパン合同会社のアカウントについては「準拠法」を日本国法、「管轄裁判所」を東京地裁と定めています。 ・AWS 環境にデプロイしたインフラストラクチャの統制に関して AWS にデプロイされている部分では、AWS が統制する物理コンポーネントを統制します。その他の部分では、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。 ・データのプライバシーと統制について AWS ではお客様のコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、お客様のコンテンツが保存される場所をお客様ご自身に決定していただき、移動中でも保管中でもコンテンツを保護し、AWS のサービスとリソースに対するユーザーからのアクセスを管理できるようにしています。また、信頼性が高く保護された技術的および物理的な制御を実施して、お客様のコンテンツに対する不正なアクセスや開示を防止しています。 ・AWS とお客様は、責任共有モデルに基づきIT 環境を統制することになります。AWS 側の責任は、安全性の高い、統制されたプラットフォームでサービスを提供し、幅広いセキュリティ機能をユーザーに提供することです。お客様の責任は、用途に合わせて安全かつ統制された方法で IT 環境を構成することにあります。ITシステムのプロプライエタリ方法にかかわらず、お客様はこれらと対し、IT 統制環境全体に対する適切な管理を維持していただく必要があります。主な実施内容として、関連資料を基にしたコンプライアンスの目標と要件の把握、その目標と要件を満たす統制環境の構築、組織のリスク許容度に基づいた必要となる妥当性の把握、統制環境の運用の有効性の検証などがあります。AWS クラウドへのデプロイにより、企業が各種の統制や検証方法を適用するにあたって選択の幅が広がります。お客様のコンプライアンスと管理が厳格な場合は、次のような基本的なアプローチも考慮可能です。このような方法でコンプライアンス管理にアプローチすることで、社内の統制環境をより理解することができます。また、実行すべき検証活動を明確にすることもできます。 1. AWS から入手できる情報、およびその他の必要な情報をレビューして IT 環境全体について可能な限り理解し、すべてのコンプライアンス要件を文書化します。 2. 企業のコンプライアンス要件を満たす統制目標を設計し、実装します。 3. 社外関係者が行う統制を特定し、文書化します 4. すべての統制目標が満たされ、すべての主な統制が設計され、その運用が有効かどうかを検証します。 ・カスタマーコンテンツの所有権と管理権について アクセス：お客様は、自分のコンテンツ、ならびに AWS のサービスとリソースへのユーザーアクセスを管理します。お客様がこれを効果的に実施できるように、AWS ではアクセス、暗号化、ログ記録の高度な機能セット（AWS CloudTrail など）を用意しています。いかなる目的であっても、当社がお客様の同意なしにお客様のコンテンツにアクセスしたり、それを使用したりすることはありません。 保存：お客様は、コンテンツを保存する AWS リージョンを選択できます。当社が、お客様の同意なしに、お客様のコンテンツをお客様が選択した AWS リージョンの外に移動したり複製したりすることはありません。セキュリティ：お客様は、自分のコンテンツの安全をどのように確保するかを選択できます。AWS では、移動中および保管中のコンテンツに対する強力な暗号化機能を利用できます。暗号化キーをお客様ご自身で管理することもできます。 カスタマーコンテンツの開示：法律、または政府機関もしくは規制機関による有効かつ拘束力のある命令を遵守するために必要な場合を除き、当社がカスタマーコンテンツを開示することはありません。開示が必要な際にも、事前の通知が禁止されている場合、または Amazon の製品もしくはサービスの使用に関連した違法行為の存在を明確に示すものがある場合を除き、Amazon はカスタマーコンテンツの開示に先立ってお客様に通知を行い、お客様が開示からの保護を求められるようにします。 セキュリティアシュアランス活動：当社は、お客様が AWS を安全に運用して AWS のセキュリティ統制環境を有効利用できるよう、グローバル/リニアプライバシーとデータ保護に関するベストプラクティスを使用したセキュリティアシュアランス活動プログラムを展開しています。これらのセキュリティ保護と管理プロセスは、複数のサードパーティによる独立した評価によって、それぞれ個別に検証されています。最新、詳細情報は 下 。 ・AWS 環境を利用している場合の監査の実施について 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。また、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。 SOX監査等の実施について お客様が AWS クラウドで会計情報を処理する場合、AWS システムの一部を Sarbanes-Oxley (SOX) の要件はほかの範囲に組み込むことについては、お客様の監査人が判断することになるでしょう。お客様の監査人は、SOX の適用可能性について独自に判断する必要があります。ほとんどの論理アクセス統制はお客様が管理するため、関連する基準に統制活動が適合しているかどうかは、お客様が判断されるのが最速です。SOX 監査人が AWS の物理的統制に関する詳細情報が必要とする場合は、SOC 1 Type II レポートを参照できます。AWS が提供する統制が詳細に記載されています。		

「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

「AWS FISCC安全対策標準対応リファレンス」からの引用					AWSの対応状況	お客様が構築すべき内容	参考情報	補足情報
標準番号	役割	対応の主体						
		AWS	お客様					
続2		-	○	-				-
続2	参考	-	○	-		<p>デジタル人材育成</p> <ul style="list-style-type: none">・マネージメント層のデジタル育成の推進に向けた知見や教訓を得ること目的とした EBC (Executive Briefing Center) という AWS のエグゼクティブや特定分野の専門家、グローバルチームと個別に具体的な話し合いをする場を提供しています。 https://aws.amazon.com/jp/executive-insights/ebc-executive-briefing-center/・AWS へのクラウドジャーニーを個人的に推進した大企業の元 CxO や上級役員をメンバーとする AWS エンタープライズストラテジストというチームがあります。チームは顧客の経営陣と協力して経験と戦略を共有し、スピードと敏捷性を高め、イノベーションを推進し、クラウドを使用して新しい運用モデルを作成し、顧客にさらに集中できるようにします。 AWS エンタープライズストラテジストについては、こちらをご参照ください。 https://aws.amazon.com/jp/executive-insights/enterprise-strategists/・AWS では、代表的なサービスやベーシックなアーキテクチャーなどの基礎コンテンツを数時間で集中的に学習できるAWS Builders Online Seriesを始め、AWS クラウドサービス活用資料集として、初心者向け資料やサービス別資料、日本版ハンズオン（初心者向けハンズオン、JP Contents Hub）を公開しており、自ら学ぶための資料や動画を多数提供しています。また、短期間で体系的に学びたいという方にはプレゼンテーションやディスカッション、実地の学習を組み合わせてすぐに役立つクラウドのスキルとベストプラクティスを教えるインストラクターによるライブ形式のAWS クラスルームトレーニング、自身の関心事に合わせて自身のペースで学習を進めたい方にはオンライン学習としてAWS Skill Builderを提供しており、クラスルームトレーニングとオンライン学習を組み合わせたブレンド型学習が可能となっています。AWS では、ロールやソリューション、業種ごとの学習ロードマップをAWS Ramp-Up Guidesとして公開しています。そして、お客様のチームと直接連携し、組織の要件に合わせたデータ駆動型のトレーニングプランを構築するAWS Learning Needs Analysis というプログラムも提供しています。- AWS Builders Online Series https://aws.amazon.com/jp/events/builders-online-series/- AWS クラウドサービス活用資料集 https://aws.amazon.com/jp/events/aws-event-resource/- 初心者向け資料 https://aws.amazon.com/jp/events/aws-event-resource/beginner/- サービス別資料 https://aws.amazon.com/jp/events/aws-event-resource/archive/- 初心者向けハンズオン https://aws.amazon.com/jp/events/aws-event-resource/hands-on/- JP Contents Hub https://aws.amazon.com/jp/contents-hub/- AWS クラスルームトレーニング https://aws.amazon.com/jp/training/classroom/- AWS Skill Builder https://aws.amazon.com/jp/training/digital/- AWS Ramp-Up Guides https://aws.amazon.com/jp/training/ramp-up-guides/- AWS Learning Needs Analysis https://aws.amazon.com/jp/training/teams/learning-needs-analysis/ <p>・AWS において学習環境を構築しやすくする仕組みとして、アカウントの分離を行うことがシンプルな方法となりますが、AWS アカウントを分離すると、複数のAWS アカウントを管理し、それぞれのAWS アカウントごとにセキュリティ設定を行い、必要に応じて最低限のリソースを事前に作成する必要があります。このようなマルチアカウント環境の運用を実現する代表的なサービスとしてAWS Organizations とAWS Control Towerがあります。AWS Organizations とAWS Control Tower を利用することで、複数のAWS アカウントを一元的に管理すると共に、一定のセキュリティ設定を揃えた環境を素早く構築でき、効率的にマルチアカウント管理を実現できます。</p> <p>・AWS では、専門家（AWS プロフェッショナルサービスやAWS/パートナー）によるサポートも提供しています。</p> <ul style="list-style-type: none">- AWS プロフェッショナルサービス https://aws.amazon.com/jp/professional-services/- AWS/パートナー https://aws.amazon.com/jp/partners/work-with-partners/		-
続3	参考	-	○	-		<p>・AWS の新サービスやアップデートの情報は、以下のサイトよりご提供しております。</p> <ul style="list-style-type: none">- AWS の最新情報 https://aws.amazon.com/jp/new/- AWS ブログ https://aws.amazon.com/jp/blogs/aws/ https://aws.amazon.com/blogs/aws/ https://aws.amazon.com/jp/blogs/news/- AWS ドキュメント（各サービスのドキュメント欄） https://docs.aws.amazon.com/ja_jp/index.html		-
続4		-	○	-				-
続5		-	○	-				-
続6		-	○	-				-
続7		-	○	-				-
続8		-	○	-				-
続9		-	○	-				-
続9	参考	-	○	-		<p>1</p> <p>・AWS では、CCoE を組成するための重要な指針としての考え方を示しています。以下をご参照ください https://aws.amazon.com/jp/blogs/news/how-to-get-started-your-own-ccoe/ https://aws.amazon.com/jp/blogs/news/how-to-define-your-own-ccoe-tasks/ https://aws.amazon.com/jp/blogs/news/steps_to_plot_ccoe/</p> <p>・お客様のクラウド導入事例として、さまざまな規模のお客様が AWS を使用して、アジリティの向上、コストの削減、そしてイノベーションの推進をクラウドで実現した方法をご紹介します。お客様のクラウド導入事例につきましては、以下のサイトをご参照ください。 https://aws.amazon.com/jp/solutions/case-studies/ctcise-jp/</p> <p>2</p> <p>・DevOps に対して、AWS がどのように役立つかをご紹介します。DevOps のリソースについては、以下をご参照ください。 https://aws.amazon.com/jp/devops/resources/</p>		-

「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

[AWS FISCS安全所高標準対応アフィリエイト]からの引用								
標準番号	役割	対応の主体		AWSの対応状況	お客様が統制すべき内容		参考情報	補足情報
		AWS	お客様					
統10		-	○	-	-	-		-
統11		-	○	-	-	-		-
統12		-	○	-	-	-		-
統13		-	○	-	-	-		-
統14		-	○	-	-	-		-
統14	参考	-	○	-	・セキュリティ教育のためのツールとして、AWS Skill Builder のAWS セキュリティラーニングプランを提供しています。 https://aws.amazon.com/jp/training/learn-about/security/ https://explore.skillbuilder.aws/learn/public/learning_plan/view/91/security-learning-plan?la=sec&sec=lp ・AWS Well-Architected Framework では、クラウド上でワークロードを設計および実行するための主要な概念、設計原則、アーキテクチャのベストプラクティスを提供しています。その中で、セキュリティの柱では、情報とシステムの保護に焦点を当てています。主なトピックには、データの機密性と完全性、ユーザー許可の管理、セキュリティイベントを検出するためのコントロールが含まれます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html		-	
統15		-	○	-	-	-		-
統15	参考	-	○	-	・AWS 認定として、基礎的な知識ベースのものから、高度な知識ベース、あるいは技術領域別の専門知識ベースの資格を設けています。 https://aws.amazon.com/jp/certification/ ・学習のためのツールとしては、個人でオンラインで取り組めるものを提供しており、複数人で参加するクラスルームやハンズオンラボといった対面参加型プログラムも提供しています。 ・AWS クラスルームトレーニング https://aws.amazon.com/jp/training/classroom/		-	
統16		-	○	-	-	-		-
統17		-	○	-	-	-		-
統18		-	○	-	-	-		-
統19		-	○	-	-	-		-
統20	1	-	○	-	-	-		-
統20	2	-	○	-	-	-		-
統20	3-(1)	-	○	-	・AWSの金融サービスに関連する情報 https://aws.amazon.com/jp/financial-services/ AWS は、銀行業務、支払い、資本市場、保険などを扱う金融サービス機関に、今日の差別化と明日のニーズに対応するために必要な、安全で回復力のあるグローバルクラウドインフラストラクチャとサービスを提供します。継続的なイノベーションを通じて、AWS は世界で最も厳しいセキュリティ要件、サービスの幅広さと深さ、深い業界の専門知識、および広範囲のパートナーネットワークを提供します。AWS 上に構築することで、組織はインフラストラクチャを近代化し、急速に変化する顧客の行動と期待に応え、ビジネスの成長を促進できます。 ・金融サービスでの導入事例 https://aws.amazon.com/jp/financial-services/customer-stories/ ・AWSの金融機関のお客様向けのセキュリティとコンプライアンスの情報 https://aws.amazon.com/jp/financial-services/security-compliance/ ・AWSのFISCに関連する情報 https://aws.amazon.com/jp/compliance/fisc/ ・AWSのPCI DSSに関連する情報 https://aws.amazon.com/jp/compliance/pci-dss-level-1-faq/ ・AWSのFinTechのセキュリティとコンプライアンスに関連する情報 https://aws.amazon.com/jp/compliance/fintech/		-	
統制環境					[概要] 「AWSとは」の全般的な説明については、「AWS とは？(注1)」を参照する。AWSを利用した導入事例に関しては、「AWS の取り組み/金融機関(注2)」「金融サービスでの導入事例(注3)」を参照する。技術レベルやプロジェクト管理といった点については「AWSのカスタマー支援(注4)」を参照する。 AWSの客観的な評価に関する第三者認証(SOCLレポート入手など)に関しては、「AWS Artifactのメトリック(注5)」 「AWS Artifactに関するよくある質問(注6)」を参照する。 [参考文献、参照URL] ○注 1 https://aws.amazon.com/jp/what-is-aws/ ホワイトペーパー「アマゾン ウェブ サービスの概要」については、以下を参照。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/aws-overview.pdf 2 https://aws.amazon.com/jp/financial-services/ 3 https://aws.amazon.com/jp/financial-services/case-studies/ 4 https://aws.amazon.com/jp/customer-enablement/ 5 https://aws.amazon.com/jp/artifact/ 6 https://aws.amazon.com/jp/artifact/faq/ ○補足(公開時期除予定) 「金融情報セキュリティに関するガイドラインが開始に該当(業種あり)された分野」現時点の記載に該当 (統20 3-(1) 記載行を参照)			
Amazon の統制環境の策定は、当社のシニアマネジメント層を起点に開始されます。役員とシニアリーダーは、当社の文化と核となる価値を確立する際、重要な役割を担っています。各従業員に当社の業務行動倫理規定が配布され、定期的なトレーニングを受けます。確立されたポリシーを従業員が理解し、従っているかどうかを確認するために、コンプライアンス監査が実施されます。AWS の組織構造が、事業運営の計画、実行、統制のフレームワークを支えています。この組織構造によって役割と責任が割り当てられ、適切な人員配置、運用の効率性、そして職務分担が構成されます。またシニアマネジメント層は、重要な人員に関する情報と適切な報告体系を構築しています。当社では従業員に対し、その職務とAWS 施設へのアクセスレベルに応じて、法律および規制が許可する範囲内での学習、雇用歴、場合によっては経歴の確認を、採用手続きの一環として実施しています。新たに採用した従業員には体系的な入社時研修を行い、Amazon のツール、プロセス、システム、ポリシー、手順について熟知させるようにします。								
リスク管理								
AWSのシニアマネジメント層は、リスクを緩和または管理するために、リスクの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、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWSの統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標 (Control Objectives for Information and related Technology, COBIT) フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO/IEC 27002 の統制に基づいたISO/IEC 27001認定フレームワーク、米国家公認会計士協会 (AICPA) のトラスト・サービスの原則 (Trust Services Principles)、PCI DSS v3.2、および米国国立標準技術研究所 (NIST) 出版物 800-53 Rev 3 (連邦政府情報システムにおける推奨セキュリティ統制) を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュ								

「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

標準番号		役割	対応の主体		AWSの対応状況	お客様が統制すべき内容	参考情報	補足情報
			AWS	お客様				
統20	3-(1)	-	○	アセットの管理 AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。 サーバーとメディアの重要な監視 ユーザーデータの保存に使用されるメディアストレージデバイスは「クリティカル」と分類されて、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。デバイスの設置、修理、および破壊（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている技法を使用してメディアを停止します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制対象です。 AWSにおけるデータプライバシー 最新、詳細情報は以下のサイトをご参照ください。 https://aws.amazon.com/jp/compliance/data-privacy-faq/ 第三者によるセキュリティ認証 AWS の第三者レポートに文書化されているように、AWS データセンターに対する第三者の検証によって、AWS がセキュリティ認証取得に必要なとなるルールを確立するためのセキュリティ対策を適切に実装していることが保証されます。コンプライアンスプログラムとその要件により、外部の監査人はメディアの廃棄のテスト、監視カメラの録画映像の確認、データセンターの入り口と通路の監視、電子アクセス制御デバイスのテスト、データセンターの機器の調査などを実施します。 ISO/IEC 27001 規格は、ISO/IEC 27002 規格のベストプラクティスカイダンスに従い、セキュリティ管理のベストプラクティスと包括的なセキュリティ統制を規定したセキュリティ管理規格です。この認証の基礎は、情報セキュリティ管理システム (ISMS) などの強固なセキュリティプログラムの開発と実装です。ISMS では、AWS がどのようにしてセキュリティを体系的で包括的な方法で継続的に管理するかを定義しています。このように広く認められている国際セキュリティ規格では、次のことが指定されています。 -情報セキュリティリスクを体系的に評価し、脅威と脆弱性の影響を考慮する -総合的な情報セキュリティ統制や他の形式のリスク管理を設計および実装し、企業およびアーキテクチャのセキュリティリスクに対処する -包括的な管理プロセスを採用し、統制により情報セキュリティのニーズが継続的に満たされるようにする AWS は ISO/IEC 27001、27017、27018 の各規格に準拠しているという認証を取得しています。これらの認証は、サードパーティの独立監査人によって実施されます。このように国際的に認められた規格および実施基準に準拠しているということは、AWS が組織のすべてのレベルで情報セキュリティに取り組んでいること、および AWS のセキュリティプログラムが業界の主なベストプラクティスに従っていることの証拠です。 最新、詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/iso-27001-faqs/ SOCレポート AWS System & Organization Control (SOC) レポートは、重要なコンプライアンス管理および目標を AWS がどのように達成したかを実証する、独立したサードパーティによる審査報告書です。このレポートの目的は、お客様とお客様の監査人が、オペレーションとコンプライアンスをサポートするよう確立された AWS 統制を簡単に把握できるようにすることです。3 種類の AWS SOC レポートがあります。 SOC 1：AWS の統制環境に関する説明、および AWS が定義した統制と目標の外部監査に関する説明 SOC 2：AWS の統制環境に関する説明と AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たす AWS 統制の外部監査に関する説明 SOC 3：AWS が AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たしていることを実証する公開レポート SOC3レポートは以下のURLからダウンロード可能です。 https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf 最新、詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/soc-faqs AWSの認証や監査レポートに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/programs/ AWSのデータセンターに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	(統20 3-(1) 記載行を参照)			
				(統20 3-(1) 記載行を参照)				
				(統20 3-(1) 記載行を参照)				
統20	3-(2)	-	○	- AWS はトップクラスのクラウドプロバイダーであり、Amazon.com の長期ビジネス戦略です。 AWSの経営方針、経営体力・収益力等については下記のURLより最新のAnnual Reportを参照ください。 https://ir.aboutamazon.com/annual-reports-proxies-and-shareholder-letters/default.aspx ・AWSの金融サービスに関連する情報 https://aws.amazon.com/jp/financial-services/ ・金融機関のAWS導入事例 https://aws.amazon.com/jp/financial-services/customer-stories/ ・AWSの金融機関のお客様向けのセキュリティとコンプライアンスの情報 https://aws.amazon.com/jp/financial-services/security-compliance/ ・AWSのFISCCに関連する情報 https://aws.amazon.com/jp/compliance/fisc/ ・AWSのPCI DSSに関連する情報 https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/ ・AWSのFinTechのセキュリティとコンプライアンスに関連する情報 https://aws.amazon.com/jp/compliance/fintech/ ビジネス継続性と災害復旧：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。 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

				「AWS FISCC安全対策基準準対応リファレンス」からの引用		AWSの対応状況		お客様が確認すべき内容		参考情報		補足情報					
標準番号	役割	対応の主体				AWS	お客様										
						第三者によるセキュリティ認証 AWS の第三者レポートに文書化されているように、AWS データセンターに対する第三者の検証によって、AWS がセキュリティ認証取得に必要なルールを確立するためのセキュリティ対策を適切に実施していることが保証されます。コンプライアンスプログラムとその要件により、外部の監査人はメディアの産量のテスト、監視カメラの録画映像の確認、データセンターの入り口と通路の監視、電子アクセス制御デバイスのテスト、データセンターの機器の調査などを実施します。 ISO/IEC 27001 規格は、ISO/IEC 27002 規格のベストプラクティスガイダンスに従い、セキュリティ管理のベストプラクティスと包括的なセキュリティ統制を規定したセキュリティ管理規格です。この認証の基礎は、情報セキュリティ管理システム (ISMS) などの強固なセキュリティプログラムの開発と実装です。ISMS では、AWS がどのようにしてセキュリティを全体的で包括的な方法で継続的に管理するかを定義しています。このように広く認められている国際セキュリティ規格では、次のことが指定されています。 -情報セキュリティリスクを体系的に評価し、脅威と脆弱性の影響を考慮する -総合的な情報セキュリティ統制や他の形式のリスク管理を設計および実装し、企業およびアーキテクチャのセキュリティリスクに対処する -包括的な管理プロセスを採用し、統制により情報セキュリティのニーズが継続的に満たされるようにする AWS は ISO/IEC 27001、27017、27018 の各規格に準拠しているという認証を取得しています。これらの認証は、サードパーティの独立監査人によって実施されます。このように国際的に認められた規格および実施基準に準拠しているということは、AWS が組織のすべてのレベルで情報セキュリティに取り組んでいること、および AWS のセキュリティプログラムが業界の主なベストプラクティスに従っていることの証拠です。最新、詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/iso-27001-faqs/ SOCレポート AWS System & Organization Control (SOC) レポートは、重要なコンプライアンス管理および目標を AWS がどのように達成したかを実証する。独立したサードパーティによる審査報告書です。このレポートの目的は、お客様とお客様の監査人が、オペレーションとコンプライアンスをサポートするよう確立された AWS 統制を簡単に把握できるようにすることです。3 種類の AWS SOC レポートがあります。 SOC 1：AWS の統制環境に関する説明、および AWS が定義した統制と目標の外部監査に関する説明 SOC 2：AWS の統制環境に関する説明と AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たす AWS 統制の外部監査に関する説明 SOC 3：AWS が AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たしていることを実証する公開レポート SOC3レポートは以下のURLからダウンロード可能です。 https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf 最新、詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/soc-faqs AWSの認証や監査レポートに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/programs/ AWSのデータセンターに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/data-center/data-centers/											
統20	3-(3)	-	○	(3)-1、2 ・データのプライバシーと統制について AWS ではお客様のコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、お客様のコンテンツが保存される場所をお客様ご自身に決定していただき、移動中でも保管中でもコンテンツを保護し、AWS のサービスとリソースに対するユーザーからのアクセスを管理できるようにしています。また、信頼性が高く連続された技術的および物理的な制御を実装して、お客様のコンテンツに対する不正なアクセスや漏示を防止しています。 カスタマーコンテンツの所有権と管理権について アクセス：お客様は、自分のコンテンツ、ならびに AWS のサービスとリソースへのユーザーアクセスを管理します。お客様がこれを効果的に実装できるように、AWS ではアクセス、暗号化、ログ記録の高度な機能セット (AWS CloudTrail など) を用意しています。いかなる目的であっても、当社がお客様の同意なくお客様のコンテンツにアクセスしたり、それを使用したりすることはありません。保存：お客様は、コンテンツを保存する AWS リージョンを選択できます。当社が、お客様の同意なしに、お客様のコンテンツをお客様が選択した AWS リージョンの外に移動したり複製したりすることはありません。 セキュリティ：お客様は、自分のコンテンツの安全をどのように確保するかを選択できます。AWS では、移動中および保管中のコンテンツに対する強力な暗号化機能を使用できます。暗号化キーをお客様ご自身で管理することもできます。カスタマーコンテンツの開示：法律、または政府機関もしくは規制機関による有効かつ相乗力のある命令を遵守するために必要な場合を除き、当社がカスタマーコンテンツを開示することはありません。開示が必要な際にも、事前の通知が禁止されている場合、または Amazon の製品もしくはサービスの使用に関連した違法行為の存在を明確に示すものがある場合を除き、Amazon はカスタマーコンテンツの開示に先立ってお客様に通知を行い、お客様が開示からの保護を求められるようにします。 セキュリティアシュアランス活動：当社は、お客様が AWS を安全に運用して AWS のセキュリティ統制環境を有効利用できるよう、グローバルなプライバシーとデータ保護に関するベストプラクティスを使用したセキュリティアシュアランス活動プログラムを展開しています。これらのセキュリティ保護と管理プロセスは、複数のサードパーティによる独立した評価によって、それぞれ個別に検証されています。最新、詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/data-privacy-faq/	(3)-1 ・AWS とお客様は、責任共有モデルに基づきIT 環境を統制することになります。AWS 側の責任は、安全性の高い、統制されたプラットフォームでサービスを提供し、幅広いセキュリティ機能をユーザーに提供することです。お客様の責任は、用途に合わせて安全かつ統制された方法で IT 環境を構成することにあります。IT システムのデプロイ方法にかかわらず、お客様はこれまでどおり、IT 統制環境全体に対する適切な管理を維持していただく必要があります。主な実施内容として、関連資料を基にしたコンプライアンスの目標と要件の把握、その目標と要件を満たす統制環境の構築、組織のリスク許容度に基づいた必要となる妥当性の把握、統制環境の運用の有効性の検証などがあります。AWS クラウドへのデプロイにより、企業が各種の統制や検証方法を適用するにあたって選択の幅が広がります。お客様のコンプライアンスと管理が厳格な場合は、次のような基本的なアプローチも考慮可能です。このような方法でコンプライアンス管理にアプローチすることで、社内の統制環境をより理解することができます。また、実行すべき検証活動を明確にすることもできます。 1. AWS から入手できる情報、およびその他の必要な情報をレビューして IT 環境全体について可能な限り理解し、すべてのコンプライアンス要件を文書化します。 2. 企業のコンプライアンス要件を満たす統制目標を設計し、実装します。 3. 社外関係者が行う統制を特定し、文書化します。 4. すべての統制目標が満たされ、すべての主な統制が設計され、その運用が有効かどうかを検証します。	[概要] AWSで提供されているサービスの可用性については、「AWSグローバルインフラストラクチャ(注1)」、「リージョンとゾーン(注2)」を参照する。 セキュリティの全般については、「AWS クラウドセキュリティ(注3)」を参照する。 個別項目に関しては下記が参考になる。 アクセス管理や認証の概要については、「アクセス管理の概要：アクセス許可とポリシー(注4)」、「AWS セキュリティ認証情報(注5)」を参照する。 環境の分離については、複数アカウントの利用による対応方法が推奨されており、「AWS マルチアカウント管理を実現するベストプラクティスとは(注6)」、および「スタートアップにおけるマルチアカウントの考え方と AWS Control Tower のすゝめ(注7)」を参照する。脆弱性の対応については、「脆弱性レポート(注8)」を参照する。 また、クラウドではオンプレと責任範囲の考え方が異なる。この点に関しては「責任共有モデル(注9)」を参照する。 [参考文献、参照URL] ○注 1 https://aws.amazon.com/jp/about-aws/global-infrastructure/ 2 https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/using-regions-availability-zones.html 3 https://aws.amazon.com/jp/security/ 4 https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/introduction_access-management.html 5 https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/security-creds.html 6 https://aws.amazon.com/jp/builders-flash/202007/multi-accounts-best-practice/ 7 https://aws.amazon.com/jp/blogs/startup/multi-accounts-and-control-tower/ 8 https://aws.amazon.com/jp/security/vulnerability-reporting/ 9 https://aws.amazon.com/jp/compliance/shared-responsibility-model/											
				(3)-4 AWS はユーザーのリソースを守るための設計と実装を行っています。また、AWSはユーザーが不正使用に対応し、その再発を防ぐための実装も行っています。・物理ネットワークにおける分離：AWSのEC2インスタンスは、物理ネットワークで分離されています。インスタンスは物理的に分離され、ネットワークは物理的に分離されています。・ネットワークの分離：AWSのネットワークインフラストラクチャは、インスタンスに対して動的にMACおよびIPアドレスを割り当て、インスタンスがそれらのアドレスのみからネットワークへ送達できるようにします。・意図のある使用との対応：AWSは、不審な行動や意図のある行動を検出し、これに対応する体制が整っています。不許可の活動は積極的に監視し、停止します。・API コールのセキュリティ：AWSの公開APIの呼び出しは、セキュリティ認証情報を使用し、署名される必要があります。・ネットワークトラフィックの制御：ユーザーは仮想プライベートクラウド(VPC)を使用して、AWSクラウド内で独自の仮想ネットワークを作成し、インフラストラクチャを分離することができます。 https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/infrastructure-security.html https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/WindowsGuide/infrastructure-security.html https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/abuse-and-compromise.html	(3)-3 AWS では、インターネット経由での利用者のアクセスに対する強固な認証を実現するため、以下のようなサービスを提供しています。利用者に対して、これらのサービスは適切に使用することで、AWSにおけるインターネット接続に対する認証強度を向上させることが可能です。 ・AWS Identity and Access Management (IAM)：IAMを使用すると、AWSリソースへのアクセスを安全に制御できます。ユーザー、グループ、および役割を作成し、それらに対して特定の権限を付与することができます。 ・Multi-Factor Authentication (MFA)：MFAは、ユーザーが自身を証明するための2つ以上の要素を要求するセキュリティシステムです。これにより、パスワードだけでなく、電話番号やハードウェアトークンなど、別の形式の認証が必要となります。 ・Amazon Cognito：Cognitoは、ユーザーのサインアップ、サインイン、アクセス制御などを管理するサービスです。Cognitoは、ソーシャルIDプロバイダ (FacebookやGoogleなど) やOpenID ConnectやSAMLなどの企業IDプロバイダを利用した認証もサポートしています。 ・AWS Key Management Service (KMS)：KMSは暗号キーの作成、制御、および管理を行うサービスで、これを利用することでデータを暗号化し、認証に関連する情報を安全に保管することができます。 ・AWS Secrets Manager：Secrets Managerは、アプリケーションのシークレット (パスワードやAPIキーなど) を安全にローテート、管理、および取得するサービスです。 ・AWS Certificate Manager：SSL/TLS証明書の取得、管理、デプロイを容易にします。これにより、AWSを使用してセキュアなネットワーク接続を確立できます。												

【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

標準番号		役割		対応の主体		AWSの対応状況	お客様が統制すべき内容	参考情報	補足情報
標準番号	役割	AWS	お客様						
統20	3-(4)	-	○	統制環境 Amazon の統制環境の策定は、当社のシニアマネジメント層を起点に開始されます。役員とシニアリーダーは、当社の文化と核となる価値を確立する際、重要な役割を担っています。各従業員に当社の業務行動倫理規定が配布され、定期的なトレーニングを受けます。確立されたポリシーを従業員が理解し、従っているかどうかを確認するために、コンプライアンス監査が実施されます。AWS の組織構造が、事業運営の計画、実行、統制のフレームワークを支えています。この組織構造によって役割と責任が割り当てられ、適切な人員調達、運用の効率性、そして職務分担が構成されます。またシニアマネジメント層は、重要な人員に関する権限と適切な報告体系を構築しています。当社では従業員に対し、その職務と AWS 施設へのアクセスレベルに応じて、法律および規制が許可する範囲内での字歴、雇用歴、場合によっては経歴の確認を、採用手続きの一環として実施しています。新たに採用した従業員には体系的な入社時研修を行い、Amazon のツール、プロセス、システム、ポリシー、手順について熟知させるようにします。 リスク管理 AWSのシニアマネジメント層は、リスクを緩和または管理するために、リスクの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、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWSの統制環境は、さまざまな内部約および外部約のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標 (Control Objectives for Information and related Technology, COBIT) フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO/IEC 27002 の統制に基づいたISO/IEC 27001認定フレームワーク、米国公認会計士協会 (AICPA) のトラスト・サービスの原則 (Trust Services Principles)、PCI DSS v3.2、および米国国立標準技術研究所 (NIST) 出版物 800-53 Rev 3 (連邦政府情報システムにおける推奨セキュリティ統制) を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に与えるセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティチームによるセキュリティ認証 AWS の第三者レポートに文書化されているように、AWS データセンターに対する第三者の検証によって、AWS がセキュリティ認証取得に必要なとなるルールを確立するためのセキュリティ対策を適切に実装していることが保証されます。コンプライアンスプログラムとその要件により、外部の監査人はメディアの偽造のテスト、監視カメラの録画映像の確認、データセンターの入り口と通路の監視、電子アクセス制御デバイスのテスト、データセンターの機器の調査などを実施します。 ISO/IEC 27001 規格は、ISO/IEC 27002 規格のベストプラクティスカイダンスに従い、セキュリティ管理のベストプラクティクスと包括的なセキュリティ統制を規定したセキュリティ管理規格です。この認証の基礎は、情報セキュリティ管理システム (ISMS) などの強固なセキュリティプログラムの開発と実装です。ISMS では、AWS がどのようにしてセキュリティを体系的で包括的な方法で継続的に管理するかを定義しています。このように広く認められている国際セキュリティ規格では、次のことが指定されています。 -情報セキュリティリスクを体系的に評価し、脅威と脆弱性の影響を考慮する -総合的な情報セキュリティ統制や他の形式のリスク管理を設計および実装し、企業およびアーキテクチャのセキュリティリスクに対処する -包括的な管理プロセスを採用し、統制により情報セキュリティのニーズが継続的に満たされるようにする AWS は ISO/IEC 27001、27017、27018 の各規格に準拠しているという認証を取得しています。これらの認証は、サードパーティの独立監査人によって実施されます。このように監査的に認められた規格および実施基準に準拠しているということは、AWS が組織のすべてのレベルで情報セキュリティに取り組んでいること、および AWS のセキュリティプログラムが業界の主なベストプラクティクスに従っていることの証拠です。最新、詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/iso-27001-faqs/ SOCレポート AWS System & Organization Control (SOC) レポートは、重要なコンプライアンス管理および目標を AWS がどのように達成したかを実証する、独立したサードパーティーによる審査報告書です。このレポートの目的は、お客様とお客様の監査人が、オペレーションとコンプライアンスをサポートするよう確立された AWS 統制を簡単に把握できるようにすることです。3 種類の AWS SOC レポートがあります。 SOC 1：AWS の統制環境に関する説明、および AWS が定義した統制と目標の外部監査に関する説明 SOC 2：AWS の統制環境に関する説明と AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たす AWS 統制の外部監査に関する説明 SOC 3：AWS が AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たしていることを実証する公開レポート SOC3レポートは以下のURLからダウンロード可能です。 https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf 最新、詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/soc-faqs AWSの認証や監査レポートに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/programs/ AWSのデータセンターに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/data-center/data-centers/					
統20	3-(5)	-	○	AWSの補助処理者、下請け業者に関する情報は以下のサイトをご参照ください。 AWS の補助処理者: https://aws.amazon.com/jp/compliance/sub-processors/ 下請け業者のアクセス: https://aws.amazon.com/jp/compliance/third-party-access/				<p>【概要】</p> <p>サービスの利用規定に関しては、「AWS カスタマーアグリーメント(注1)」「AWS のサービス条件(注2)」を参照する。また、リスク・コンプライアンスの全般に関しては、ホワイトペーパー「アマゾン ウェブ サービス: リスクとコンプライアンス(注3)」、「コンプライアンスに関するよくある疑問(注4)」を参照する。(補足 上記ホワイトペーパー中に注記されているが(注5)、最新版については「コンプライアンスのリソース(注6)」を参照する。)</p> <p>再委託先の情報に関しては、「AWSの補助処理者(注7)」、「下請け業者のアクセス(注8)」が参考になる。障害時等における対策に関しては、「日本の災害対策関連情報(注9)」が参考になる。</p> <p>【参考文献、参照URL】</p> <p>○注</p> <p>1 https://aws.amazon.com/jp/agreement/</p> <p>2 https://aws.amazon.com/jp/service-terms/</p> <p>3 https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf</p> <p>4 https://aws.amazon.com/jp/compliance/faq/</p> <p>5 http://aws.amazon.com/compliance/aws-whitepapers/</p> <p>6 (注をアクセスすると転送される) https://aws.amazon.com/jp/compliance/resources/</p> <p>7 https://aws.amazon.com/jp/compliance/sub-processors/</p> <p>8 https://aws.amazon.com/jp/compliance/third-party-access/</p> <p>9 https://aws.amazon.com/jp/compliance/jp-dr-considerations/</p>	

【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

「AWS FISCC安全計画基準対応リファレンス」おらの引用						
標準番号	役割	対応の主体		AWSの対応状況	お客様が統制すべき内容	参考情報
		AWS	お客様			
統20	3-(6)	-	○	<p>・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提供した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。AWSの法務関連の情報は以下のサイトをご参照ください。また、契約、その他法務関連のお問い合わせについては担当営業までご連絡ください。</p> <p>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査または検証は、一般的に、統制の証明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、お客様の主要な統制を AWS が管理している場合でも、統制目標と統制の設計と運用効率のまま維持し、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お客様にも役立ちます。</p> <p>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情報は、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。</p>	-	<p>【概要】</p> <p>本項目については、AWSが直接実施している対策というよりは、AWSが提供する機能を前提に、それらの機能を用いて金融機関側が実施する対策となっており、その参考となる情報を記載する。 サービスの利用規定に関しては、「AWS カスタマーアグリメント(注1)」「AWS のサービス条件(注2)」を参照する。個別事項では下記が参考になる。</p> <p>AWS のセキュリティ、コンプライアンスサービスについては、「AWS のセキュリティ、アイデンティティ、コンプライアンス(注3)」に関連する各サービス上のリンクが示されており、S3 サービスにおける暗号化については、「暗号化によるデータの保護(注4)」を参照する。各サービスにおける暗号化のサポート状況については、「AWS のサービスのプライバシー機能(注5)」に各サービスへのリンクが示されている。モニタリングとログ記録に関しては、「AWS のコンプライアンスツール(注6)」を参照する。バックアップ/リストアに関しては、「バックアップと復元(注7)」を参照する。ネットワークの設定・セキュリティに関するFAQについては、「AWS Answers ネットワーキング(注8)」を参照する。</p> <p>【参考文献、参照URL】</p> <p>○注</p> <ol style="list-style-type: none">1 https://aws.amazon.com/jp/agreement/2 https://aws.amazon.com/jp/service-terms/3 https://aws.amazon.com/jp/products/security/4 https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/UsingEncryption.html5 https://aws.amazon.com/jp/compliance/data-privacy/service-capabilities/6 https://aws.amazon.com/jp/compliance/compliance-tools/7 https://aws.amazon.com/jp/backup-restore/8 https://aws.amazon.com/jp/answers/networking/
統20	3-(7)	-	○	<p>SOCレポート</p> <p>AWS System & Organization Control (SOC) レポートは、重要なコンプライアンス管理および目標を AWS がどのように達成したかを裏証する、独立したサードパーティーによる審査報告書です。このレポートの目的は、お客様とお客様の監査人が、オペレーションとコンプライアンスをサポートするよう確立された AWS 統制を簡単に把握できるようにすることです。3 種類の AWS SOC レポートがあります。</p> <p>SOC 1：AWS の統制環境に関する説明、および AWS が定義した統制と目標の外部監査に関する説明</p> <p>SOC 2：AWS の統制環境に関する説明と AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たす AWS 統制の外部監査に関する説明</p> <p>SOC 3：AWS が AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たしていることを裏証する公開レポート</p> <p>SOC3レポートは以下のURLからダウンロード可能です。 https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf 最新。詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/soc-faqs</p> <p>AWSの認証や監査レポートに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/programs/ AWSのデータセンターに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/data-center/data-centers/</p>	-	<p>【概要】</p> <p>AWSの訪問調査のスタンス(訪問を許可していない)については、「主要なコンプライアンスに関する質問と AWS の回答(注1)」の「データセンター訪問」を参照する。 AWSのデータセンターのコントロールについては、「AWSのコントロール(注2)」を参照する。SOCレポートに関しては、「SOC(注3)」を参照する。</p> <p>【参考文献、参照URL】</p> <p>○注</p> <ol style="list-style-type: none">1 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Answers_to_Key_Compliance_Questions_JP.pdf2 https://aws.amazon.com/jp/compliance/data-center/controls/3 https://aws.amazon.com/jp/compliance/soc-faqs
統20	3-(8)	-	○	<p>・AWSでは既存システムとの連携・新システムへのデータ移行を容易にするサービスを提供しています。以下はサービスの例です。</p> <p>- AWS Storage Gateway Storage Gateway は、お客様によるオンプレミスアプリケーションを AWS ストレージにシームレスに接続して拡張します。お客様は、Storage Gateway を使うことで、テープライブラリのクラウドストレージへの置き換え、クラウドストレージによるファイル共有の実施、および、オンプレミスアプリケーションが AWS 内のデータにアクセスするための低レイテンシーキャッシュの作成などが、シームレスに行えます。</p> <p>- AWS Database Migration Service AWS Database Migration Service を使用すると、データベースを短期間で安全に AWS に移行できます。移行中でもソースデータベースは完全に利用可能な状態に保たれ、データベースを利用するアプリケーションのダウンタイムを最小限に抑えられます。</p> <p>- AWS Direct Connect Direct Connect の物理的な専用接続を使用すると、社内データセンターと AWS のデータセンターの間のネットワーク転送速度を上げることができます。</p> <p>AWS Direct Connect では、お客様のネットワークと AWS Direct Connect のいずれかのロケーションとの間に専用のネットワーク接続を確立することができます。</p> <p>- AWS DataSync AWS DataSync は、オンプレミスストレージと Amazon S3、Amazon Elastic File System (Amazon EFS) または Amazon FSx for Windows ファイルサーバーとの間でデータの移動を簡単に自動化するデータ転送サービスです。</p> <p>- AWS Transfer Family AWS Transfer Family は、Amazon S3 との間で直接ファイル転送を実行できるように、フルマネージド型のサポートを提供します。Secure File Transfer Protocol (SFTP)、File Transfer Protocol over SSL (FTPS)、および File Transfer Protocol (FTP) をサポートする AWS Transfer Family では、既存の認証システムと連携し、Amazon Route 53 を使用した DNS ルーティングを提供することにより、ファイル転送ワークフローを AWS にシームレスに移行できるようにします。</p> <p>クラウドへのデータ移行を支援するサービスの詳細については以下を参照ください。 https://aws.amazon.com/jp/cloud-data-migration/</p>	-	<p>【概要】</p> <p>本基準で記述されている移行の容易性の評価の参考になるように、AWSでの移行について、移行方式と移行目的の例を補足する。</p> <p>【例】</p> <p>AWSでは、移行方式の例として以下の6つを挙げています。(6R)</p> <ul style="list-style-type: none">・ Rehost OSやアプリケーションに変更を加えずそのまま移行・ Replatform OSまたはDBの変更やアップグレード・ Repurchase アプリケーションの買い替え・ Refactor 移行時にクラウドネイティブなアプリケーションへ書き換え・ Retire オンプレ環境でサーバ(やアプリケーション)を廃止する・ Retain オンプレ環境で引き続き運用する <p>移行目的の例として、「コストダウン」「耐障害性」「アジリティ」「運用負荷の低減」「グローバル展開」「イノベーションの加速」が挙げられており、目的に適した移行方式を検討する。</p> <p>【参考文献、参照URL】</p> <ul style="list-style-type: none">・ 【AWS White Belt Online Seminar】クラウドジャーニー https://d1.awsstatic.com/webinars/jp/pdf/services/20180417_AWS-BlackBelt_CloudJourney.pdf <p>(統20 3-(8) 記載行を参照)</p>
統20	3-(9)	-	○	<p>・AWS サポートでは、現在の、または今後予定されているユースケースに基づき、AWS でのみ可能なツールと専門知識の組み合わせによって、適切な成果が得られるようお客様をサポートします。</p> <p>AWSサポートの詳細については下記の情報を参照ください。 https://aws.amazon.com/jp/premiumsupport/</p> <p>また、技術的なお問い合わせについては日本語でのお問い合わせにも対応いたします。詳細については以下の情報を参照ください。 https://aws.amazon.com/jp/premiumsupport/tech-support-guidelines/</p>	-	<p>【概要】</p> <p>保守体制・サポート体制については、「AWSサポート(注1)」で、ビジネスサポート、エンタープライズサポートのプランが紹介されている。利用時のエンジニアによる24時間365日のサポート提供の方針が示されており、各プランの詳細は「AWSビジネスサポート(注2)」「AWS エンタープライズサポート(注3)」を参照する。料金については、「AWS サポートのプランの料金(注4)」を参照する。サポートに関する詳細ドキュメントについては、「AWS Support のドキュメント(注5)」を参照する。</p> <p>【参考文献、参照URL】</p> <p>○注</p> <ol style="list-style-type: none">1 https://aws.amazon.com/jp/premiumsupport/2 https://aws.amazon.com/jp/premiumsupport/plans/business/3 https://aws.amazon.com/jp/premiumsupport/plans/enterprise/4 https://aws.amazon.com/jp/premiumsupport/pricing/5 https://docs.aws.amazon.com/ja_jp/aws-support/

【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

「AWS FISCC安全対策基準 対応リファレンス」からの引用							
標準番号	役割	対応の主体		AWSの対応状況	お客様が読解すべき内容	参考情報	補足情報
		AWS	お客様				
統20	3-(10)	-	○	<ul style="list-style-type: none">・AWSの法務関連の情報は以下のサイトをご参照ください。 https://aws.amazon.com/jp/legal/ また、契約、その他法務関連のお問い合わせについては担当営業までご連絡ください。・AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです・AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます・AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます・AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです	-	<p>【概要】</p> <p>契約の全体的な詳細については、AWS カスタマーアグリーメント(注1)を参照する。AWS カスタマーアグリーメントの[第11条 責任限定]にアマゾン側の責任について記載されている(注2)。</p> <p>(補足)日本語翻訳版と英語版に差異がある場合、英語版が優先するので注意。</p> <p>また、サービスレベルアグリーメント(SLA)に関しては、AWS サービスレベルアグリーメント(注3)を参照する。</p> <p>【参考文献、参照URL】</p> <p>○注</p> <p>1 https://aws.amazon.com/jp/agreement/</p> <p>2 注1のリンクより日本語版アクセス可能</p> <p>3 https://aws.amazon.com/jp/legal/service-level-agreements/</p>	-
統20	3-(11)	-	○	<ul style="list-style-type: none">・AWS ではコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、自分のコンテンツをどこに保存するかをお客様に決定していただき、転送中のコンテンツと保管中のコンテンツを保護し、お客様のユーザーの AWS のサービスとリソースに対するアクセスを管理できるようにしています。また、お客様のコンテンツに対する不正アクセスや開示を防止するよう設計された、洗練された信頼性の高い技術的および物理的な管理を実践しています。 https://aws.amazon.com/jp/compliance/data-privacy-faq/ <p>データの容量や種類が増えるにつれ、データの保存、保護、復元はますます難しい課題となってきました。AWS のツールやリソースを利用すると、スケーラビリティ、耐久性、安全性に優れたバックアップと復元のソリューションを構築して、現在、使用している機能を強化または変換することができます。お客様の復旧時間目標 (RTO)、復旧ポイント目標 (RPO)、データ維持要件、各種コンプライアンス要件を満たすために、AWS と AWS のストレージパートナーのエコシステムをご活用ください。従量課金制のため、先行投資は必要ありません。オンプレミス型、ハイブリッド型、クラウドネイティブ型など、IT 環境のタイプにかかわらず、お客様のニーズを満たすデータ保護ソリューションを設計およびデプロイできます。 https://aws.amazon.com/jp/backup-restore/</p> <p>アセットの管理</p> <p>AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。</p> <p>メディアの破壊ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通して非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および廃棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。</p> <p>AWSの認証や監査レポートに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/programs/ AWSのデータセンターに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/data-center/data-centers/</p>	-	<p>【概要】</p> <p>AWSの契約終了に関しては、「AWS アカウントを解約する方法を教えてください(注1)」を参照する。</p> <p>【参考文献、参照URL】</p> <p>○注</p> <p>1 https://aws.amazon.com/jp/premiumsupport/knowledge-center/close-aws-account/</p> <p>(統20 3-(11) 記載行を参照)</p>	-
統20	3-(12)	-	○	<ul style="list-style-type: none">・AWS ではカスタマーコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、自分のコンテンツがどこに保存されるかをお客様ご自身に決定していただき、移動中でも保管中でもコンテンツを保護し、AWS のサービスとリソースに対するユーザーからのアクセスを管理できるようにしています。また、カスタマーコンテンツに対する不正なアクセスや開示を防止するよう設計された、洗練された信頼性の高い技術的および物理的な管理を実践しています。 https://aws.amazon.com/jp/compliance/data-privacy-faq/	-	<p>【概要】</p> <p>クラウド内のカスタマーコンテンツに含まれる個人データに関しては、金融機関等側の責任となる。</p> <p>AWS側の関連する対応に関して、データブライ/シー全般については、「データブライ/シーのよくある質問(注1)」を参照する。クラウド上の個人データ保護の規格(ISO 27018)については、「ISO/IEC 27018:2019 コンプライアンス(注2)」を参照する。</p> <p>【参考文献、参照URL】</p> <p>○注</p> <p>1 https://aws.amazon.com/jp/compliance/data-privacy-faq/</p> <p>2 https://aws.amazon.com/jp/compliance/iso-27018-faqs/</p>	-
統20	3-(13)	-	○	<ul style="list-style-type: none">・AWS では 200 種類を超えるクラウドサービスについて従量制料金を適用しています。AWS では必要な個々のサービスにのみ、サービスを使用する期間だけお支払いいただき、長期契約や複雑なライセンスは必要ありません。 サービスを消費した分だけ支払い、サービスの使用を停止したときの追加コストや解約料金はありません。 https://aws.amazon.com/jp/pricing/	-	<p>【概要】</p> <p>サービス料金については、「AWSの料金(注1)」に概要があり、従量制料金を基本にすることが示されている。見積りについては、「AWS料金見積りツール(注2)」が利用可能である。構成と料金試算の例については、「目的別 クラウド構成と概算料金例(注3)」を参照する。</p> <p>【例】</p> <p>サービス別に料金体系は提示されており、各サービスで代表的なものとして、コンピューティング「Amazon EC2料金」(注4)、ストレージ「Amazon S3の料金」(注5)、データベース「Amazon RDSの料金」(注6)に関する記述は、下記URLを参照する。またサポートプランについては、「AWS サポートのプランの料金(注7)」を参照する。</p> <p>【参考文献、参照URL】</p> <p>○注</p> <p>1 https://aws.amazon.com/jp/pricing/</p> <p>2 https://calculator.aws/#/</p> <p>3 https://aws.amazon.com/jp/cdp/</p> <p>4 https://aws.amazon.com/jp/ec2/pricing/</p> <p>5 https://aws.amazon.com/jp/s3/pricing/</p> <p>6 https://aws.amazon.com/jp/rds/pricing/</p> <p>7 https://aws.amazon.com/jp/premiumsupport/pricing/</p>	-
統20	3-(14)		○	<ul style="list-style-type: none">・AWSのカスタマーアグリーメントにおいて、クラウドサービスの販売者がアマゾン ウェブ サービス ジャパン合同会社のアカウントについては「準拠法」を日本国法、「管轄裁判所」を東京地裁と定めています。	-	<p>【概要】</p> <p>契約の全体的な詳細については、AWS カスタマーアグリーメント(注1)を参照する。上記には、日本準拠法に関するカスタマーアグリーメント変更契約に関する注釈が記載されている。当該契約にアクセスするにはAWSコンソール(注2)へのログインが必要となる。</p> <p>【参考文献、参照URL】</p> <p>○注</p> <p>1 https://aws.amazon.com/jp/agreement/</p> <p>2 https://console.aws.amazon.com/artifact</p>	-
統20	4	-	○	-	-	-	-
統20	5	-	○	-	-	-	-
統20	6	-	○	-	-	-	-

「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

標準番号		対応の主体		「AWS FISCC安全対策基準 対応リファレンス」からの引用		お客様が統制すべき内容		参考情報		補足情報	
		AWS	お客様	AWSの対応状況							
統21	1, 2	-	○	・契約時に考慮すべき事項の例としてご参照ください。 AWSの法務関連の情報は以下のサイトをご参照ください。 https://aws.amazon.com/jp/legal/ また、契約、その他法務関連のお問い合わせについては担当営業までご連絡ください - AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです - AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます - AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます - AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです ・AWSのカスタマーアグリーメントにおいて、クラウドサービスの販売者がアマゾン ウェブ サービス ジャパン合同会社のアカウントについては「準拠法」を日本国法、「管轄裁判所」を東京地裁と定めています。	-		-				
統21	1-(6)	-	○	・契約時に考慮すべき事項の例としてご参照ください。 AWSの法務関連の情報は以下のサイトをご参照ください。 https://aws.amazon.com/jp/legal/ また、契約、その他法務関連のお問い合わせについては担当営業までご連絡ください。 - AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです - AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます - AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます - AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです ・AWSのカスタマーアグリーメントにおいて、クラウドサービスの販売者がアマゾン ウェブ サービス ジャパン合同会社のアカウントについては「準拠法」を日本国法、「管轄裁判所」を東京地裁と定めています。	-		-				
統21	1-(11)	-	○	AWSでは、個人データが含まれる可能性のあるコンテンツなど、お客様がAWSにアップロードされたコンテンツにアクセス可能な下請け業者について、お客様に事前に通知いたします。お客様がAWSにアップロードしたお客様の所有のコンテンツへのアクセスをAWSが承認している下請け業者はありません。下請け業者のアクセスを常時監視するには、AWSサードパーティーによるアクセスのウェブページをご参照ください。 https://aws.amazon.com/jp/compliance/third-party-access AWS は、お客様の代わりに特定の処理活動を行うため、または、データセンター施設の管理アクティビティを行うため、AWS 補助処理者のウェブページにリストされている事業者を従事させることがあります。 https://aws.amazon.com/jp/compliance/sub-processors/	-		-				
統21	1-(12)	-	○	・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、検証するのににも有用です。AWSの法務関連の情報は以下のサイトをご参照ください。また、契約、その他法務関連のお問い合わせについては担当営業までご連絡ください。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 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 レポートの一端として、独立し、資格を持つ監査人が統制の有効と運用を検証しています。この点に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率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相関の検証も、ISO/IEC 27001 監査、PCI 評価、ITAR 監査、FedRAMP テストプログラム	-		-				
統21	1-(13)	-	○	・契約時に考慮すべき事項の例としてご参照ください。 AWSの法務関連の情報は以下のサイトをご参照ください。 https://aws.amazon.com/jp/legal/ また、契約、その他法務関連のお問い合わせについては担当営業までご連絡ください。 - AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです - AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます - AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます - AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです ・AWSのカスタマーアグリーメントにおいて、クラウドサービスの販売者がアマゾン ウェブ サービス ジャパン合同会社のアカウントについては「準拠法」を日本国法、「管轄裁判所」を東京地裁と定めています。	-		-				
統21	1-(14)	-	○	AWS の第三者レポートに文書化されているように、AWS データセンターに対する第三者の検証によって、AWS がセキュリティ認証取得に必要なルールを確立するためのセキュリティ対策を適切に実装していることが保証されます。コンプライアンスプログラムとその要件により、外部の監査人はメディアの廃棄のテスト、監視カメラの録画映像の確認、データセンターの入り口と通路の監視、電子アクセス制御デバイスのテスト、データセンターの機器の調査などを実施します。	-		-				
統21	3, 4	-	○	-	-		-				

「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

「AWS FISCC安全対策基準 対応リファレンス」おらの引用						
基準番 号	役割	対応の主体		AWSの対応状況	お客様が統制すべき内容	参考情報
		AWS	お客様			
統22	1	-	○	<p>- AWSの法務関連の情報は以下のサイトをご参照ください。 https://aws.amazon.com/jp/legal/ また、契約、その他法務関連のお問い合わせについては担当営業までご連絡ください。</p> <p>- AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです</p> <p>- AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます</p> <p>- AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます</p> <p>- AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです</p> <p>AWS 環境にデプロイしたインフラストラクチャの統制に関して</p> <p>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、接続ポイントや送達の統制を含め、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。</p> <p>AWS 環境を利用している場合の監査の実施について</p> <p>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。また、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に使用できます。</p> <p>SOX監査等の実施について</p> <p>お客様が AWS クラウドで会計情報を処理する場合、AWS システムの一部を Sarbanes-Oxley (SOX) の要件の範囲に組み込むことについては、お客様の監査人が判断することになるでしょう。お客様の監査人は、SOX の適用可能性について独自に判断する必要があります。ほとんどの論理アクセス統制はお客様が管理するため、関連する基準に統制活動が適合しているかどうかは、お客様が判断されるのが最適です。SOX 監査人が AWS の物理的統制に関する詳細情報を必要とする場合は、SOC 1 Type II レポートを参照できます。AWS が提供する統制が詳細に記載されています。</p> <p>お客様のデータセンター訪問</p> <p>AWS のデータセンターは多数のお客様をホストしており、そうした様々なお客様が第三者による物理的なアクセスに曝されることになってしまいうため、お客様によるデータセンター訪問を許可しておりません。このようなデータセンターに関するお客様のニーズを満たすために、SOC 1 Type II レポートの取り組みの一つとして、独立し、資格を持つ監査人がそのような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第三者による検証によって、お客様は運用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 1Type II レポートのコピーを要求できます。また、データセンターの物理的なセキュリティの個別の確認についても、ISO/IEC 27001 監査、PCI 評価、ITAR 監査、FedRAMP 等のテストプログラムの一部となっています。</p> <p>従業員へのセキュリティ教育、トレーニング</p> <p>AWSでは従業員へのセキュリティ訓練やアプリケーションへのセキュリティレビューを含む、セキュリティポリシーを定めています。これらにより、データに対する機密性、完全性、可用性をアセスするとともに、情報セキュリティポリシーとの準拠性についても検証します。社員が様々な役割と責任を理解するのを助けるため、ISO/IEC 27001規格に準拠した、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。</p> <p>第三者によるセキュリティ認証</p> <p>AWS の第三者レポートに文書化されているように、AWS データセンターに対する第三者の検証によって、AWS がセキュリティ認証取得に必要となるルールを確立するためのセキュリティ対策を適切に実装していることが保証されます。コンプライアンスプログラムとその要件により、外部の監査人はメディアの機密のテスト、監視カメラの録画映像の確認、データセンターの入り口と通路の監視、電子アクセス制御デバイスのテスト、データセンターの機器の調査などを実施します。</p> <p>ISO/IEC 27001 規格は、ISO/IEC 27002 規格のベストプラクティスガイダンスに従い、セキュリティ管理のベストプラクティスと包括的なセキュリティ統制を規定したセキュリティ管理規格です。この認証の基礎は、情報セキュリティ管理システム (ISMS) などの強固なセキュリティプログラムの開発と実装です。ISMS では、AWS がどのようにしてセキュリティを全体で包括的な方法で継続的に管理するかを定義しています。このように広く認められている国際セキュリティ規格では、次のことが指定されています。</p> <p>-情報セキュリティリスクを体系的に評価し、脅威と脆弱性の影響を考慮する</p> <p>-総合的な情報セキュリティ統制や他の形式のリスク管理を設計および実装し、企業およびアーキテクチャのセキュリティリスクに対処する</p> <p>-包括的な管理プロセスを採用し、統制により情報セキュリティのニーズが継続的に満たされるようにする</p> <p>AWS は ISO/IEC 27001、27017、27018 の各規格に準拠しているという認証を取得しています。これらの認証は、サードパーティの独立監査人によって実施されます。このように定期的に認められた規格および実施基準に準拠していることは、AWS が組織のすべてのレベルで情報セキュリティに取り組んでいること、および AWS のセキュリティプログラムが業界の主なベストプラクティスに従っていることの証拠です。最新、詳細情報は下記のサイトをご参照ください。 https://aws.amazon.com/jp/compliance/iso-27001-faqs/</p>	<p>【概要】</p> <p>金融機関側ではデータセンターなどの状況を直接確認することは困難なため、第三者保証による報告書の確認などで代替する必要がある。契約の全体については、「AWS カスタマーアグリーメント(注1)」、「AWS のサービス条件(注2)」を参照する。SOCレポートに関しては、「SOC(注3)」を参照する。AWSのデータセンターのコントロールについては、「AWSのコントロール(注4)」を参照する。ISO27001系の認証の取得状況については、「ISO および CSA STAR 認証(注5)」を参照する。</p> <p>【参考文献、参照URL】</p> <p>○注</p> <p>1 https://aws.amazon.com/jp/agreement/ 2 https://aws.amazon.com/jp/service-terms/ 3 https://aws.amazon.com/jp/compliance/soc-faqs 4 https://aws.amazon.com/jp/compliance/data-center/controls/ 5 https://aws.amazon.com/jp/compliance/iso-certified/</p> <p>(統22 1 記載行を参照)</p> <p>(統22 1 記載行を参照)</p>	-

「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

標準番号 技術		対応の主体			AWSの対応状況	お客様が統制すべき内容		参考情報	補足情報
		AWS	お客様						
統22	2	-	○		SOCレポート AWS System & Organization Control (SOC) レポートは、重要なコンプライアンス管理および目標を AWS がどのように達成したかを実証する。独立したサードパーティによる審査報告書です。このレポートの目的は、お客様とお客様の監査人が、オペレーションとコンプライアンスをサポートするよう確立された AWS 統制を簡単に把握できるようにすることです。3 種類の AWS SOC レポートがあります。 SOC 1：AWS の統制環境に関する説明、および AWS が定義した統制と目標の外部監査に関する説明 SOC 2：AWS の統制環境に関する説明と AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たす AWS 統制の外部監査に関する説明 SOC 3：AWS が AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たしていることを実証する公開レポート SOC3レポートは以下のURLからダウンロード可能です。 https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf 最新、詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/soc-faqs AWSの認証や監査レポートに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/programs/ AWSのデータセンターに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	-	(統22 1 記載行を参照)		
	統22	3	-	○		SOCレポート AWS System & Organization Control (SOC) レポートは、重要なコンプライアンス管理および目標を AWS がどのように達成したかを実証する。独立したサードパーティによる審査報告書です。このレポートの目的は、お客様とお客様の監査人が、オペレーションとコンプライアンスをサポートするよう確立された AWS 統制を簡単に把握できるようにすることです。3 種類の AWS SOC レポートがあります。 SOC 1：AWS の統制環境に関する説明、および AWS が定義した統制と目標の外部監査に関する説明 SOC 2：AWS の統制環境に関する説明と AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たす AWS 統制の外部監査に関する説明 SOC 3：AWS が AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たしていることを実証する公開レポート SOC3レポートは以下のURLからダウンロード可能です。 https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf 最新、詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/soc-faqs AWSの認証や監査レポートに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/programs/ AWSのデータセンターに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	-	[概要] 金融機関側ではデータセンターなどの状況を直接確認することは困難なため、第三者保証による報告書の確認などで代替する必要がある。SOCレポートに関しては、「SOC[注1)」を参照する。 [参考文献、参照URL] ○注 1 https://aws.amazon.com/jp/compliance/soc-faqs	-
統22	4	-	○		第三者によるセキュリティ認証 AWS の第三者レポートに文書化されているように、AWS データセンターに対する第三者の検証によって、AWS がセキュリティ認証取得に必要となるルールを確立するためのセキュリティ対策を適切に実施していることが保証されます。コンプライアンスプログラムとその要件により、外部の監査人はメディアの徹底的なテスト、監視カメラの録画映像の確認、データセンターの入り口と通路の監視、電子アクセス制御デバイスのテスト、データセンターの機器の調査などを実施します。 ISO/IEC 27001 規格は、ISO/IEC 27002 規格のベストプラクティスカイダンスに従い、セキュリティ管理のベストプラクティクスと包括的なセキュリティ統制を規定したセキュリティ管理規格です。この認証の基礎は、情報セキュリティ管理システム (ISMS) などの強固なセキュリティプログラムの開発と実装です。ISMS では、AWS がどのようにしてセキュリティを体系的で包括的な方法で継続的に管理するかを定義しています。このように広く認められている国際セキュリティ規格では、次のことが指定されています。-情報セキュリティリスクを体系的に評価し、脅威と脆弱性の影響を考慮する -包括的な情報セキュリティ統制や他の形式のリスク管理を設計および実装し、企業およびアーキテクチャのセキュリティリスクに対処する -包括的な管理プロセスを採用し、統制により情報セキュリティのニーズが継続的に満たされるようにする。 AWS は ISO/IEC 27001、27017、27018 の各規格に準拠しているという認証を取得しています。これらの認証は、サードパーティの独立監査人によって実施されます。このように国際的に認められた規格および実施基準に準拠していることは、AWS が組織のすべてのレベルで情報セキュリティに取り組んでいること、および AWS のセキュリティプログラムが業界の主なベストプラクティクスに従っていることの証拠です。最新、詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/iso-27001-faqs/	-	[概要] 金融機関側ではデータセンターなどの状況を直接確認することは困難なため、第三者保証による報告書の確認などで代替する必要がある。SOCレポートに関しては、「SOC[注1)」を参照する。 [参考文献、参照URL] ○注 1 https://aws.amazon.com/jp/compliance/soc-faqs	-	

「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

標準番号	役割	対応の主体		AWSの対応状況	お客様が統制すべき内容	参考情報	補足情報
		AWS	お客様				
統23	1, 2	-	○	<p>AWSの法務関連の情報は以下のサイトをご参照ください。 https://aws.amazon.com/jp/legal/ また、契約、その他法務関連のお問い合わせについては担当営業までご連絡ください。</p> <p>- AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです</p> <p>- AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます</p> <p>- AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます</p> <p>- AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです</p> <p>AWS 環境にデプロイしたインフラストラクチャの統制に関して</p> <p>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。</p> <p>AWS 環境を利用している場合の監査の実施について</p> <p>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。また、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。</p> <p>SOX監査等の実施について</p> <p>お客様が AWS クラウドで会計情報を処理する場合、AWS システムの一部を Sarbanes-Oxley (SOX) の要件の範囲に組み込むことについては、お客様の監査人が判断することになるでしょう。お客様の監査人は、SOX の適用可能性について独自に判断する必要があります。ほとんどの論理アクセス統制はお客様が管理するため、関連する基準に統制活動が適合しているかどうかは、お客様が判断されるのが最適です。SOX 監査人が AWS の物理的統制に関する詳細情報が必要とする場合は、SOC 1 Type II レポートを参照できます。AWS が提供する統制が詳細に記載されています。</p> <p>お客様のデータセンター訪問</p> <p>AWS のデータセンターは多数のお客様をホストしており、そうした様々なお客様が第三者による物理的なアクセスに曝されることになってしまうため、お客様によるデータセンター訪問を許可しておりません。このようなデータセンターに関するお客様のニーズを満たすために、SOC 1 Type II レポートの取り組みの一つとして、独立し、資格を持つ監査人がそのような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第三者による検証によって、お客様は運用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 1Type II レポートのコピーを要求できます。また、データセンターの物理的なセキュリティの個別の確認についても、ISO/IEC 27001 監査、PCI 評価、ITAR 監査、FedRAMP 等のテストプログラムの一部となっています。</p> <p>第三者によるセキュリティ認証</p> <p>AWS の第三者レポートに文書化されているように、AWS データセンターに対する第三者の検証によって、AWS がセキュリティ認証取得に必要なとなるルールを確立するためのセキュリティ対策を適切に実装していることが保証されます。コンプライアンスプログラムとその要件により、外部の監査人はメディアの廃棄のテスト、監視カメラの録画映像の確認、データセンターの入り口と通路の監視、電子アクセス制御デバイスのテスト、データセンターの機器の調査などを実施します。</p> <p>ISO/IEC 27001 規格は、ISO/IEC 27002 規格のベストプラクティスガイダンスに従い、セキュリティ管理のベストプラクティスと包括的なセキュリティ統制を規定したセキュリティ管理規格です。この認証の基礎は、情報セキュリティ管理システム (ISMS) などの強固なセキュリティプログラムの開発と実装です。ISMS では、AWS がどのようにしてセキュリティを体系的で包括的な方法で継続的に管理するかを定義しています。このように広く認められている国際セキュリティ規格では、次のことが指定されています。</p> <p>- 情報セキュリティリスクを体系的に評価し、脅威と脆弱性の影響を考慮する</p> <p>- 総合的な情報セキュリティ統制や他の形式のリスク管理を設計および実装し、企業およびアーキテクチャのセキュリティリスクに対処する</p> <p>- 包括的な管理プロセスを採用し、統制により情報セキュリティのニーズが継続的に満たされるようになる</p> <p>AWS は ISO/IEC 27001、27017、27018 の各規格に準拠しているという認証を取得しています。これらの認証は、サードパーティの独立監査人によって実施されます。このように国際的に認められた規格および実施基準に準拠しているということは、AWS が組織のすべてのレベルで情報セキュリティに取り組んでいること、および AWS のセキュリティプログラムが業界の主なベストプラクティスに従っていることの証拠です。</p> <p>最新、詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/iso-27001-faqs/</p> <p>SOC1レポート</p> <p>AWS System & Organization Control (SOC) レポートは、重要なコンプライアンス管理および目標を AWS がどのように達成したかを実証する、独立したサードパーティによる審査報告書です。このレポートの目的は、お客様とお客様の監査人が、オペレーションとコンプライアンスをサポートするよう確立された AWS 統制を簡単に把握できるようにすることです。3 種類の AWS SOC レポートがあります。</p> <p>SOC 1：AWS の統制環境に関する説明、および AWS が定義した統制と目標の外部監査に関する説明</p> <p>SOC 2：AWS の統制環境に関する説明と AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たす AWS 統制の外部監査に関する説明</p> <p>SOC 3：AWS が AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たしていることを実証する公開レポート</p> <p>SOC3レポートは以下のURLからダウンロード可能です。 https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf 最新、詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/soc-faqs</p> <p>AWSの認証や監査レポートに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/programs/ AWSのデータセンターに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/data-center/data-centers/</p>	<p>【概要】</p> <p>金融機関側ではデータセンターなどの状況を直接確認することは困難なため、第三者保証による報告書の確認などで代替する必要がある。SOC1レポートに関しては、「SOC(注1)」を参照する。AWSのデータセンターのコントロールについては、「AWSのコントロール(注2)」を参照する。AWSのSLAに関しては、「AWS サービスレベルアグリーメント(注3)」を参照する。</p> <p>【参考文献、参照URL】</p> <p>○注</p> <p>1 https://aws.amazon.com/jp/compliance/soc-faqs</p> <p>2 https://aws.amazon.com/jp/compliance/data-center/controls/</p> <p>3 https://aws.amazon.com/jp/legal/service-level-agreements/</p> <p>(統23 1,2 記載行を参照)</p> <p>(統23 1,2 記載行を参照)</p> <p>(統23 1,2 記載行を参照)</p>		

【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

標準番号				「AWS FISCC安全計画基準対応リファレンス」からの引用		お客様が統制すべき内容		参考情報		補足情報	
標準番号	役割	対応の主体	対応状況	AWSの対応状況	お客様が統制すべき内容	参考情報	補足情報				
統23	3	-	○	<p>SOCレポート</p> <p>AWS System & Organization Control (SOC) レポートは、重要なコンプライアンス管理および目標を AWS がどのように達成したかを実証する、独立したサードパーティによる審査報告書です。このレポートの目的は、お客様とお客様の監査人が、オペレーションとコンプライアンスをサポートするよう確立された AWS 統制を簡単に把握できるようにすることです。3 種類の AWS SOC レポートがあります。</p> <p>SOC 1：AWS の統制環境に関する説明、および AWS が定義した統制と目標の外部監査に関する説明</p> <p>SOC 2：AWS の統制環境に関する説明と AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たす AWS 統制の外部監査に関する説明</p> <p>SOC 3：AWS が AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たしていることを実証する公開レポート</p> <p>SOC3レポートは以下のURLからダウンロード可能です。</p> <p>https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf</p> <p>最新、詳細情報は下記のサイトを参照ください。</p> <p>https://aws.amazon.com/jp/compliance/soc-faqs</p> <p>AWSの認証や監査レポートに関する 詳細情報は下記を参照ください。</p> <p>https://aws.amazon.com/jp/compliance/programs/</p> <p>AWSのデータセンターに関する 詳細情報は下記を参照ください。</p> <p>https://aws.amazon.com/jp/compliance/data-center/data-centers/</p>	-	<p>【概要】</p> <p>金融機関側ではデータセンターなどの状況を直接確認することは困難なため、第三者保証による報告書の確認などで代替する必要がある。SOCレポートに関しては、「SOC[注1]」を参照する。AWSのデータセンターのコントロールについては、「AWSのコントロール[注2]」を参照する。AWSのSLAに関しては、「AWS サービスレベルアグリーメント[注3]」を参照する。</p> <p>【参考文献、参照URL】</p> <p>○注</p> <p>1 https://aws.amazon.com/jp/compliance/soc-faqs</p> <p>2 https://aws.amazon.com/jp/compliance/data-center/controls/</p> <p>3 https://aws.amazon.com/jp/legal/service-level-agreements/</p>					
統24	1	-	○	<p>・以下の各項目は、リスクベースでお客様固有のクラウドサービスに関連する統制を考慮する際の情報として参照ください。</p> <p>AWSとお客様は、責任共有モデルに基づきIT 環境を統制することになります。AWS 側の責任は、安全性の高い、統制されたプラットフォームでサービスを提供し、幅広いセキュリティ機能をユーザーに提供することです。お客様の責任は、用途に合わせて安全かつ統制された方法で IT 環境を構成することにあります。ITシステムのデプロイ方法にかかわらず、お客様はこれまでどおり、IT 統制環境全体に対する適切な管理を維持していただく必要があります。主な実施内容として、関連資料を基にしたコンプライアンスの目標と要件の把握、その目標と要件を満たす統制環境の構築、組織のリスク許容度に基づいた必要となる妥当性の把握、統制環境の運用の有効性の検証などがあります。AWS クラウドへのデプロイにより、企業が各種の統制や検証方法を適用するにあたって選択の幅が広がります。お客様のコンプライアンスと管理が厳格な場合は、次のような基本的なアプローチも考慮可能です。このような方法でコンプライアンス管理にアプローチすることで、社内の統制環境をより理解することができます。また、実行すべき検証活動を明確にすることもできます。</p> <p>1. AWS から入手できる情報、およびその他の必要な情報をレビューして IT 環境全体について可能な限り理解し、すべてのコンプライアンス要件を文書化します。</p> <p>2. 企業のコンプライアンス要件を満たす統制目標を設計し、実装します。</p> <p>3. 社外関係者が行う統制を特定し、文書化します。</p> <p>4. すべての統制目標が満たされ、すべての主な統制が設計され、その運用が有効かどうかを検証します。</p> <p>AWSの法務関連の情報は以下のサイトをご参照ください。</p> <p>https://aws.amazon.com/jp/legal/</p> <p>また、契約、その他法務関連のお問い合わせについては担当営業までご連絡ください。</p> <p>- AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです</p> <p>- AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます</p> <p>- AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます</p> <p>- AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです</p> <p>- AWSのカスタマーアグリーメントにおいて、クラウドサービスの販売者がアマゾン ウェブ サービス ジャパン合同会社のアカウントについては「準拠法」を日本国法、「管轄裁判所」を東京地裁と定めています。</p> <p>- AWS 環境にデプロイしたインフラストラクチャの統制に関して</p> <p>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ピューターネットワークを統制します。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。</p> <p>・データのプライバシーと統制について</p> <p>AWS ではお客様のコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、お客様のコンテンツが保存される場所をお客様ご自身に決定していただき、移動中でも保管中でもコンテンツを保護し、AWS のサービスとリソースに対するユーザーからのアクセスを管理できるようにしています。また、信頼性が高く洗練された技術的および物理的な制御を実装して、お客様のコンテンツに対する不正なアクセスや開示を防止しています。</p> <p>カスタマーコンテンツの所有権と管理権について</p> <p>アクセス: お客様は、自分のコンテンツ、ならびに AWS のサービスとリソースへのユーザーアクセスを管理します。お客様がこれを効果的に実施できるように、AWS ではアクセス、暗号化、ログ記録の高度な機能セット (AWS CloudTrail など) を用意しています。いかなる目的であっても、当社がお客様の同意なしにお客様のコンテンツにアクセスしたり、それを使用したりすることはありません。</p> <p>保存: お客様は、コンテンツを保存する AWS リージョンを選択できます。当社が、お客様の同意なしに、お客様のコンテンツをお客様が選択した AWS リージョンの外に移動したり複製したりすることはありません。</p> <p>セキュリティ: お客様は、自分のコンテンツの安全をどのように確保するかを選択できます。AWS では、移動中および保管中のコンテンツに対する強力な暗号化機能を利用できます。暗号化キーをお客様ご自身で管理することもできます。</p> <p>カスタマーコンテンツの開示: 法律、または政府機関もしくは規制機関による有効かつ拘束力のある命令を遵守するために必要な場合を除き、当社がカスタマーコンテンツを開示することはありません。開示が必要な際にも、事前の通知が禁止されている場合、または Amazon の製品もしくはサービスの使用に関連した違法行為の存在を明確に示すものがある場合を除き、Amazon はカスタマーコンテンツの開示に先立ってお客様に通知を行い、お客様が開示からの保護を求められるようにします。</p> <p>セキュリティアラザランス活動: 当社は、お客様 が AWS を安全に運用して AWS のセキュリティ統制環境を有効利用できるよう、グローバル/IL なプライバシーとデータ保護に関するベストプラクティスを使用したセキュリティアラザランス活動プログラムを展開しています。これらのセキュリティ保護と管理プロセスは、複数のサードパーティによる独立した評価によって、それぞれ個別に検証されています。</p> <p>最新、詳細情報は下記を参照ください。</p> <p>https://aws.amazon.com/jp/compliance/data-privacy-faq/</p> <p>AWS 環境を利用している場合の監査の実施について</p> <p>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。また、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。</p>	-	<p>【概要】</p> <p>利用中の AWS アカウントに適用されている準拠法・管轄裁判所の日本法・東京地方裁判所への変更は、金融機関等自身で行うことが可能。AWS のコンプライアンスレポートにオンデマンドでアクセスできる無料のセルフサービスポータル「AWS Artifact[注1]」を通じ、「日本準拠法に関する AWS カスタマーアグリーメント変更契約」を有効化する。以下のサイトに変更方法、操作方法が掲載されている。</p> <p>また、統制対象クラウド拠点に関する情報としては、「グローバルインフラストラクチャ[注2]」が参考になる。</p> <p>【参考文献、参照URL】</p> <p>○注</p> <p>1 https://aws.amazon.com/jp/artifact/ https://aws.amazon.com/jp/artifact/getting-started/</p> <p>2 https://aws.amazon.com/jp/about-aws/global-infrastructure/</p> <p>(統24 1 記載行を参照)</p> <p>(統24 1 記載行を参照)</p>					

【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

				[AWS FISCC安全対策基準対応リファレンス]からの引用				お客様が統制すべき内容		参考情報		補足情報	
標準番号	技術	対応の主体		AWSの対応状況									
		AWS	お客様										
統24	2		○	-	SOX監査等の実施について						(統24 1 記載行を参照)		
					お客様が AWS クラウドで会計情報を処理する場合、AWS システムの一部を Sarbanes-Oxley (SOX) の要件の範囲に組み込むことについては、お客様の監査人が判断することになるでしょう。お客様の監査人は、SOX の適用可能性について独自に判断する必要があります。ほとんどの論理アクセス統制はお客様が管理するため、関連する基準に統制活動が適合しているかどうかは、お客様が判断されるのが最適です。SOX 監査人が AWS の物理的統制に関する詳細情報を必要とする場合は、SOC 1 Type II レポートを参照できます。AWS が提供する統制が詳細に記載されています。								
					お客様のデータセンター訪問								
					AWS のデータセンターは多数のお客様をホストしており、そうした様々なお客様が第三者による物理的なアクセスに与えられることになってしまいます。お客様によるデータセンター訪問を許可しておりません。このようなデータセンターに関するお客様のニーズを満たすために、SOC 1 Type II レポートの取り組みの一つとして、独立し、資格を持つ監査人がそのような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第三者による検証によって、お客様は適用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 1Type II レポートのコピーを要求できます。また、データセンターの物理的なセキュリティの徹底的な確認についても、ISO/IEC 27001 監査、PCI 評価、ITAR 監査、FedRAMP等のテストプログラムの一部となっています。								
					第三者によるセキュリティ認証								
					AWS の第三者レポートに文書化されているように、AWS データセンターに対する第三者の検証によって、AWS がセキュリティ認証取得に必要なルールを確立するためのセキュリティ対策を適切に実装していることが保証されます。コンプライアンスプログラムとその要件により、外部の監査人はメディアの産業のテスト、監視カメラの録画映像の確認、データセンターの入り口と通路の監視、電子アクセス制御デバイスのテスト、データセンターの機器の調査などを実施します。								
					ISO/IEC 27001 規格は、ISO/IEC 27002 規格のベストプラクティスガイダンスに従い、セキュリティ管理のベストプラクティスと包括的なセキュリティ統制を規定したセキュリティ管理規格です。この認証の基礎は、情報セキュリティ管理システム (ISMS) などの強固なセキュリティプログラムの開発と実装です。ISMS では、AWS がどのようにしてセキュリティを体系的で包括的な方法で継続的に管理するかを定義しています。このように広く認められている国際セキュリティ規格では、次のことが指定されています。								
					-情報セキュリティリスクを体系的に評価し、脅威と脆弱性の影響を考慮する								
					-総合的な情報セキュリティ統制や他の形式のリスク管理を設計および実装し、企業およびアーキテクチャのセキュリティリスクに対処する								
					-包括的な管理プロセスを採用し、統制により情報セキュリティのニーズが継続的に満たされるようにする								
					AWS は ISO/IEC 27001、27017、27018 の各規格に準拠しているという認証を取得しています。これらの認証は、サードパーティの独立監査人によって実施されます。このように国際的に認められた規格および実施基準に準拠しているということは、AWS が組織のすべてのレベルで情報セキュリティに取り組んでいること、および AWS のセキュリティプログラムが業界の主なベストプラクティスに従っていることの証据です。最新、詳細情報は下記のサイトを参照ください。								
					https://aws.amazon.com/jp/compliance/iso-27001-faqs/								
					SOCレポート								
					AWS System & Organization Control (SOC) レポートは、重要なコンプライアンス管理および目標を AWS がどのように達成したかを実証する、独立したサードパーティによる審査報告書です。このレポートの目的は、お客様とお客様の監査人が、オペレーションとコンプライアンスをサポートするよう確立された AWS 統制を簡単に把握できるようにすることです。3 種類の AWS SOC レポートがあります。								
					SOC 1：AWS の統制環境に関する説明、および AWS が定義した統制と目標の外部監査に関する説明								
					SOC 2：AWS の統制環境に関する説明と AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たす AWS 統制の外部監査に関する説明								
					SOC 3：AWS が AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たしていることを実証する公開レポート								
					SOC3レポートは以下のURLからダウンロード可能です。								
					https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf								
					最新、詳細情報は下記のサイトを参照ください。								
					https://aws.amazon.com/jp/compliance/soc-faqs								
					AWSの認証や監査レポートに関する 詳細情報は下記を参照ください。								
					https://aws.amazon.com/jp/compliance/programs/								
					AWSのデータセンターに関する 詳細情報は下記を参照ください。								
					https://aws.amazon.com/jp/compliance/data-center/data-centers/								

「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

「AWS FISCC安全対策基準対応リファレンス」おらの引用					参考情報	補足情報
標準番号	技術	対応の主体		AWSの対応状況		
		AWS	お客様		お客様が統制すべき内容	
				<p>・AWSのカスタマーアグリーメントにおいて、クラウドサービスの販売者がアマゾン ウェブ サービス ジャパン合同会社のアカウントについては「準拠法」を日本国法、「管轄裁判所」を東京地裁と定めています。</p> <p>・AWS 環境にデプロイしたインフラストラクチャの統制に関して 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、接続ポイントや送値の統制を含め、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。</p> <p>・データのプライバシーと統制について AWS ではお客様のコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、お客様のコンテンツが保存される場所をお客様ご自身に決定していただき、移動中でも保管中でもコンテンツを保護し、AWS のサービスとリソースに対するユーザーからのアクセスを管理できるようにしています。また、信頼性が高く洗練された技術的および物理的な制御を実装して、お客様のコンテンツに対する不正なアクセスや開示を防止しています。</p> <p>カスタマーコンテンツの所有権と管理権について アクセス：お客様は、自分のコンテンツ、ならびに AWS のサービスとリソースへのユーザーアクセスを管理します。お客様がこれを効果的に実装できるように、AWS ではアクセス、暗号化、ログ記録の高度な機能セット (AWS CloudTrail など) を用意しています。いかなる目的であっても、当社がお客様の同意なしにお客様のコンテンツにアクセスしたり、それを使用したりすることはありません。 保存：お客様は、コンテンツを保存する AWS リージョンを選択できます。当社が、お客様の同意なしに、お客様のコンテンツをお客様が選択した AWS リージョンの外に移動したり複製したりすることはありません。 セキュリティ：お客様は、自分のコンテンツの安全をどのように確保するかを選択できます。AWS では、移動中および保管中のコンテンツに対する強力な暗号化機能を利用できます。暗号化キーをお客様ご自身で管理することもできます。 カスタマーコンテンツの開示：法律、または政府機関もしくは規制機関による有効かつ拘束力のある命令を遵守するために必要な場合を除き、当社がカスタマーコンテンツを開示することはありません。開示が必要な際にも、事前の通知が禁止されている場合、または Amazon の製品もしくはサービスの使用に関連した違法行為の存在を明確に示すものがある場合を除き、Amazon はカスタマーコンテンツの開示に先立ってお客様に通知を行い、お客様が開示からの保護を求められるようにします。 セキュリティシミュレーション活動：当社は、お客様が AWS を安全に運用して AWS のセキュリティ統制環境を有効利用できるよう、グローバルなプライバシーとデータ保護に関するベストプラクティスを使用したセキュリティシミュレーション活動プログラムを展開しています。これらのセキュリティ保護と管理プロセスは、複数のサードパーティによる独立した評価によって、それぞれ個別に検証されています。 最新、詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/data-privacy-faq/</p> <p>AWS 環境を利用している場合の監査の実施について 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。また、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に使用できます。 SOX監査等の実施について お客様が AWS クラウドで会計情報を処理する場合、AWS システムの一部を Sarbanes-Oxley (SOX) の要件の範囲に組み込むことについては、お客様の監査人が判断することになるでしょう。お客様の監査人は、SOX の適用可能性について独自に判断する必要があります。ほとんどの論理アクセス統制はお客様が管理するため、関連する基準に統制活動が適合しているかどうかは、お客様が判断されるのが最適です。SOX 監査人が AWS の物理的統制に関する詳細情報が必要とする場合は、SOC 1 Type II レポートを参照できます。AWS が提供する統制が詳細に記載されています。</p> <p>お客様のデータセンター訪問 AWS のデータセンターは多数のお客様をホストしており、そうした様々なお客様が第三者による物理的なアクセスに曝されることになってしまいうため、お客様によるデータセンター訪問を許可していません。このようなデータセンターに関するお客様のニーズを満たすために、SOC 1 Type II レポートの取り扱ひの一つとして、独立し、資格を持つ監査人がそのような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第三者による検証によって、お客様は運用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 1Type II レポートのコピーを要求できます。また、データセンターの物理的なセキュリティの個別の統制についても、ISO/IEC 27001 監査、PCI 評価、ITAR 監査、FedRAMP 等のデスタプログラムの一部となっています。</p> <p>第三者によるセキュリティ認証 AWS の第三者レポートに文書化されているように、AWS データセンターに対する第三者の検証によって、AWS がセキュリティ認証取得に必要なとなるルールを確立するためのセキュリティ対策を適切に実装していることが保証されます。コンプライアンスプログラムとその要件により、外部の監査人はメディアの廃棄のテスト、監視カメラの録画映像の確認、データセンターの入り口と通路の監視、電子アクセス制御デバイスのテスト、データセンターの機器の調査などを実施します。</p> <p>ISO/IEC 27001 規格は、ISO/IEC 27002 規格のベストプラクティスガイダンスに従い、セキュリティ管理のベストプラクティスと包括的なセキュリティ統制を規定したセキュリティ管理規格です。この認証の基礎は、情報セキュリティ管理システム (ISMS) などの強固なセキュリティプログラムの開発と実装です。ISMS では、AWS がどのようにしてセキュリティを全体で包括的な方法で継続的に管理するかを定義しています。このように広く認められている国際セキュリティ規格では、次のことが指定されています。 ・情報セキュリティリスクを体系的に評価し、脅威と脆弱性の影響を考慮する ・総合的な情報セキュリティ統制や他の形式のリスク管理を設計および実装し、企業およびアーキテクチャのセキュリティリスクに対処する ・包括的な管理プロセスを採用し、統制により情報セキュリティのニーズが継続的に満たされるようにする</p> <p>AWS は ISO/IEC 27001、27017、27018 の各規格に準拠しているという認証を取得しています。これらの認証は、サードパーティの独立監査人によって実施されます。このように国際的に認められた規格および実施基準に準拠しているということは、AWS が組織のすべてのレベルで情報セキュリティに取り組んでいること、および AWS のセキュリティプログラムが業界の主なベストプラクティスに従っていることの証です。最新、詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/iso-27001-faq/</p>	(統24 2 記載行を参照)	
						(統24 2 記載行を参照)
						(統24 2 記載行を参照)
						(統24 2 記載行を参照)

「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

「AWS FISCC安全対策基準対応リファレンス」からの引用					参考情報	
標準番号	役割	対応の主体		AWSの対応状況	お客様が統制すべき内容	参考情報
		AWS	お客様			補足情報
				<p>SOCレポート</p> <p>AWS System & Organization Control (SOC) レポートは、重要なコンプライアンス管理および目標を AWS がどのように達成したかを実証する、独立したサードパーティによる審査報告書です。このレポートの目的は、お客様とお客様の監査人が、オペレーションとコンプライアンスをサポートするよう確立された AWS 統制を簡単に把握できるようにすることです。3 種類の AWS SOC レポートがあります。</p> <p>SOC 1：AWS の統制環境に関する説明、および AWS が定義した統制と目標の外部監査に関する説明 SOC 2：AWS の統制環境に関する説明と AICPA の信頼サービスセキュリティ、可用性、機密性、プライバシーの基準を満たす AWS 統制の外部監査に関する説明 SOC 3：AWS が AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たしていることを実証する公開レポート</p> <p>SOC3レポートは以下のURLからダウンロード可能です。 https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf 最新、詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/soc-faqs</p> <p>AWSの認証や監査レポートに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/programs/ AWSのデータセンターに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/in/compliance/data-center/data-centers/</p> <p>AWSとお客様は、責任共有モデルに基づきIT環境を統制することになります。AWS側の責任は、安全性の高い、統制されたプラットフォームでサービスを提供し、幅広いセキュリティ機能をユーザーに提供することです。お客様の責任は、用途に合わせて安全かつ統制された方法でIT環境を構成することにあります。ITシステムのデプロイ方法にかかわらず、お客様はこれまでどおり、IT統制環境全体に対する適切な管理を維持していただく必要があります。主な実施内容として、関連資料を基にしたコンプライアンスの目標と要件の把握、その目標と要件を満たす統制環境の構築、組織のリスク許容度に基づいた必要となる妥当性の把握、統制環境の運用の有効性の検証などがあります。AWS クラウドへのデプロイにより、企業が各種の統制や検証方法を適用するにあたって選択の幅が広がります。お客様のコンプライアンスと管理が厳格な場合は、次のような基本的なアプローチも考慮可能です。このような方法でコンプライアンス管理にアプローチすることで、社内の統制環境をより理解することができます。また、実行すべき検証活動を明確にすることもできます。</p> <p>1. AWSから入手できる情報、およびその他の必要な情報をレビューしてIT環境全体について可能な限り理解し、すべてのコンプライアンス要件を文書化します。 2. 企業のコンプライアンス要件を満たす統制目標を設計し、実装します。 3. 社外関係者が行う統制を特定し、文書化します。 4. すべての統制目標が満たされ、すべての主要な統制が設計され、その運用が有効かどうかを検証します。</p> <p>AWS環境にデプロイしたインフラストラクチャの統制に関して</p> <p>AWSにデプロイされている部分では、AWSが提供する物理コンポーネントを統制します。その他の部分は、接続ポイントや送達の統制を含め、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ISO/IEC 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</p> <p>AWS環境を利用している場合の監査の実施について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。また、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。</p> <p>SOX法の監査について</p> <p>お客様が AWS クラウドで会計情報を処理する場合、AWS システムの一部を Sarbanes-Oxley (SOX) の要件の範囲に組み込むことについては、お客様の監査人が判断することになるでしょう。お客様の監査人は、SOX の適用可能性について独自に判断する必要があります。ほとんどの論理アクセス統制はお客様が管理するため、関連する基準に統制活動が適合しているかどうかは、お客様が判断されるのが最良です。SOX 監査人がAWS の物理的統制に関する詳細情報が必要とする場合は、SOC 1 Type II レポートを参照できます。AWS が提供する統制が詳細に記載されています。</p> <p>お客様のデータセンター訪問</p> <p>AWS のデータセンターは多数のお客様をホストしており、そうした様々なお客様が第三者による物理的なアクセスに曝されることになってしまつため、お客様によるデータセンター訪問を許可しておりません。このようにデータセンターに関するお客様のニーズを満たすために、SOC 1 Type II レポートの取り扱ひの一つとして、独立し、資格を持つ監査人がそのような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第三者による検証によって、お客様は運用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 1Type II レポートのコピーを要求できます。また、データセンターの物理的なセキュリティの個別の確認についても、ISO/IEC 27001 監査、PCI 評価、ITAR 監査、FedRAMP等のテストプログラムの一部となっています。</p> <p>第三者によるセキュリティ認証</p> <p>AWS の第三者レポートに文書化されているように、AWS データセンターに対する第三者の検証によって、AWS がセキュリティ認証取得に必要なルールを確立するためのセキュリティ対策を適切に実装していることが保証されます。コンプライアンスプログラムとその要件により、外部の監査人はメディアの廃棄のテスト、監視カメラの録画映像の確認、データセンターの入り口と通路の監視、電子アクセス制御デバイスのテスト、データセンターの機器の調査などを実施します。</p> <p>ISO/IEC 27001 規格は、ISO/IEC 27002 規格のベストプラクティスガイダンスに従い、セキュリティ管理のベストプラクティスと包括的なセキュリティ統制を規定したセキュリティ管理規格です。この認証の基礎は、情報セキュリティ管理システム (ISMS) などの強固なセキュリティプログラムの開発と実行です。ISMSはしばしばセキュリティを全体的で包括的な方法で体系的に管理する方法を定義しています。このように広く認められている国際セキュリティ規格では、次のことが指定されています。<情報セキュリティリスクを体系的に評価し、脅威と脆弱性の影響を考慮する-包括的な情報セキュリティ統制や他の形式のリスク管理を設計および実装し、企業およびアプリケーションのセキュリティリスクに対処する-包括的な管理プロセスを採用し、統制により情報セキュリティのニーズが継続的に満たされるようにする</p> <p>AWS は ISO/IEC 27001、27017、27018の各規格に準拠しているという認証を取得しています。これらの認証は、サードパーティの独立監査人によって実施されます。このように国際的に認められた規格および実施基準に準拠しているということは、AWSが組織のすべてのレベルで情報セキュリティに取り組んでいること、およびAWSのセキュリティプログラムが業界の主なベストプラクティスに従っていることの証拠です。最新、詳細情報は下記のサイトを参照ください。https://aws.amazon.com/jp/compliance/iso-27001-faqs/</p>	(註24 2 記載行を参照)	

「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

「AWS FISCC安全対策基準対応リファレンス」おらの引用						
標準番 号	改訂	対応の主体		AWSの対応状況	お客様が統制すべき内容	参考情報
		AWS	お客様			
統24	4	-	○	<p>・AWSとお客様は、責任共有モデルに基づきIT 環境を統制することになります。AWS 側の責任は、安全性の高い、統制されたプラットフォームでサービスを提供し、幅広いセキュリティ機能をユーザーに提供することです。お客様側の責任は、用途に合わせて安全かつ統制された方法で IT 環境を構成することにあります。IT システムのデプロイ方法にかかわらず、お客様はこれまでどおり、IT 統制環境全体に対する適切な管理を維持していただく必要があります。主な実施内容として、関連資料を基にしたコンプライアンスの目標と要件の把握、その目標と要件を満たす統制環境の構築、組織のリスク許容度に基づいた必要となる妥当性の把握、統制環境の運用の有効性の検証などがあります。AWS クラウドへのデプロイにより、企業が各種の統制や検証方法を適用するにあたって選択の幅が広がります。お客様のコンプライアンスと管理が厳格な場合は、次のような基本的なアプローチも考慮可能です。このような方法でコンプライアンス管理にアプローチすることで、社内の統制環境をより理解することができます。また、実行すべき検証活動を明確にすることもできます。</p> <p>1. AWS から入手できる情報、およびその他の必要な情報をレビューして IT 環境全体について可能な限り理解し、すべてのコンプライアンス要件を文書化します。</p> <p>2. 企業のコンプライアンス要件を満たす統制目標を設計し、実装します。</p> <p>3. 社外関係者が行う統制を特定し、文書化します。</p> <p>4. すべての統制目標が満たされ、すべての主な統制が設計され、その運用が有効かどうかを検証します。</p> <p>AWS 環境にデプロイしたインフラストラクチャの統制に関して</p> <p>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（SMP）および AWS の実装は、SOX Type II レポートを要求できます。</p> <p>AWS 環境を利用している場合の監査の実施についてほとんどのレイヤーと、物理統制より上の統制の監査は、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。また、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。</p> <p>SOX法の監査について</p> <p>お客様が AWS クラウドで会計情報を処理する場合、AWS システムの一部を Sarbanes-Oxley (SOX) の要件の範囲に組み込むことについては、お客様の監査人が判断することになるでしょう。お客様の監査人は、SOX の適用可能性について独自に判断する必要があります。ほとんどの論理アクセス統制はお客様が管理するため、関連する基準に統制活動が適合しているかどうかは、お客様が判断されるのが最適です。SOX 監査人が AWS の物理的統制に関する詳細情報が必要とする場合は、SOC 1 Type II レポートを参照できます。AWS が提供する統制が詳細に記載されています。</p> <p>お客様のデータセンター訪問</p> <p>AWS のデータセンターは多数のお客様をホストしており、そうした様々のお客様が第三者による物理的なアクセスに曝されることになってしまいうため、お客様によるデータセンター訪問を許可しておりません。このようなデータセンターに関するお客様のニーズを満たすために、SOC 1 Type II レポートの取り組みの一つとして、独立し、資格を持つ監査人がそのような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第三者による検証によって、お客様は運用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。また、データセンターの物理的なセキュリティの個別の確認についても、ISO/IEC 27001 監査、PCI 評価、ITAR 監査、FedRAMP等のテストプログラムの一部となっています。</p> <p>第三者によるセキュリティ認証</p> <p>AWS の第三者レポートに文書化されているように、AWS データセンターに対する第三者の検証によって、AWS がセキュリティ認証取得に必要なとなるルールを確立するためのセキュリティ対策を適切に実装していることが保証されます。コンプライアンスプログラムとその要件により、外部の監査人はメディアの産業のテスト、監視カメラの録画映像の確認、データセンターの入り口と通路の監視、電子アクセス制御デバイスのテスト、データセンターの機器の調査などを実施します。</p> <p>ISO/IEC 27001 規格は、ISO/IEC 27002 規格のベストプラクティスガイダンスに従い、セキュリティ管理のベストプラクティスと包括的なセキュリティ統制を規定したセキュリティ管理規格です。この認証の基盤は、情報セキュリティ管理システム (ISMS) などの強固なセキュリティプログラムの開発と実装です。ISMS では、AWS がどのようにしてセキュリティを体系的で包括的な方法で継続的に管理するかを定義しています。このように広く認められている国際セキュリティ規格では、次のことが指定されています。</p> <p>・情報セキュリティリスクを体系的に評価し、脅威と脆弱性の影響を考慮する</p> <p>・総合的な情報セキュリティ統制や他の形式のリスク管理を設計および実装し、企業およびアーキテクチャのセキュリティリスクに対処する</p> <p>・包括的な管理プロセスを採用し、統制により情報セキュリティのニーズが継続的に満たされるようにする</p> <p>AWS は ISO/IEC 27001、27017、27018 の各規格に準拠しているという認証を取得しています。これらの認証は、サードパーティの独立監査人によって実施されます。このように国際的に認められた規格および実施基準に準拠しているということは、AWS が組織のすべてのレベルで情報セキュリティに取り組んでいること、および AWS のセキュリティプログラムが業界の主なベストプラクティスに従っていることの証です。最新、詳細情報は下記のサイトを参照ください。</p> <p>https://aws.amazon.com/jp/compliance/iso-27001-faqs/</p> <p>SOC レポート</p> <p>AWS System & Organization Control (SOC) レポートは、重要なコンプライアンス管理および目標を AWS がどのように達成したかを実証する、独立したサードパーティによる審査報告書です。このレポートの目的は、お客様とお客様の監査人が、オペレーションとコンプライアンスをサポートするよう確立された AWS 統制を簡単に把握できるようにすることです。3 種類の AWS SOC レポートがあります。</p> <p>SOC 1：AWS の統制環境に関する説明、および AWS が定義した統制と目標の外部監査に関する説明</p> <p>SOC 2：AWS の統制環境に関する説明と AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たす AWS 統制の外部監査に関する説明</p> <p>SOC 3：AWS が AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たしていることを実証する公開レポート</p> <p>SOC3レポートは以下のURLからダウンロード可能です。</p> <p>https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf</p> <p>最新、詳細情報は下記のサイトを参照ください。</p> <p>https://aws.amazon.com/jp/compliance/soc-faqs</p> <p>AWSの認証や監査レポートに関する 詳細情報は下記を参照ください。</p> <p>https://aws.amazon.com/jp/compliance/programs/</p> <p>AWSのデータセンターに関する 詳細情報は下記を参照ください。</p> <p>https://aws.amazon.com/is/compliance/data-center/data-centers/</p>	<p>[概要]</p> <p>SOC3レポートはAWS公式サイト[注1]から、SOC1/SOC2レポートは、AWS のコンプライアンスレポートにオンデマンドでアクセスできる無料のセルフサービスポータル「AWS Artifact[注2]」から入手できる。</p> <p>SOC1/SOC2レポート利用に際しては、利用(を予定)しているリージョンおよびサービスがレポートのスコープに含まれているか、参照しているSOCレポートが直近のものであるかを確認する。</p> <p>また、SOC1/SOC2レポートに限らず、Artifactからダウンロードした文書に記載のTERMS AND CONDITIONSからの逸脱に注意する(秘密情報としての取扱い等)。</p> <p>[参考文献、参照URL]</p> <p>○注</p> <p>1 https://aws.amazon.com/jp/compliance/soc-faqs/ https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf</p> <p>2 https://aws.amazon.com/jp/artifact/ https://aws.amazon.com/jp/artifact/getting-started/</p> <p>(統24 4 記載行を参照)</p> <p>(統24 4 記載行を参照)</p> <p>(統24 4 記載行を参照)</p>	-

【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

標準番号		役割		対応の主体		AWSの対応状況		お客様が統制すべき内容		参考情報		補足情報		
				AWS		お客様								
統24	5	-		○		・AWSとお客様は、責任共有モデルに基づきIT 環境を統制することになります。AWS 側の責任は、安全性の高い、統制されたプラットフォームでサービスを提供し、幅広いセキュリティ機能をユーザーに提供することです。お客様側の責任は、用途に合わせて安全かつ統制された方法で IT 環境を構成することにあります。IT システムのデプロイ方法にかかわらず、お客様はこれまでも、IT 統制環境全体に対する適切な管理を維持していただく必要があります。主な実施内容として、関連資料を基にしたコンプライアンスの目標と要件の把握、その目標と要件を満たす統制環境の構築、組織のリスク許容度に基づいた必要となる妥当性の把握、統制環境の運用の有効性の検証などがあります。AWS クラウドへのデプロイにより、企業が各種の統制や検証方法を適用するにあたって選択の幅が広がります。お客様のコンプライアンスと管理が最優先の場合は、次のような基本的なアプローチも考慮可能です。このような方法でコンプライアンス管理にアプローチすることで、社内の統制環境をより理解することができます。また、実行すべき検証活動を明確にすることもできます。				【概要】 金融機関等側ではAWS の論理統制と物理統制を直接確認することは困難なため、第三者による監査報告書による確認などで代替する必要がある。これらを定期的に入手・内容を確認する方法で、監査の実施が可能となる。 AWSのアカウントを取得すると、AWS の全てのコンプライアンスレポートにオンデマンドでアクセスできる無料のセルフサービスポータル「AWS Artifact(注1)」が利用可能となる。AWS 監査人が発行したレポートや、SOC2やPCIDSS等のサードパーティによる証明のダウンロードが可能(注2)で、金融機関等の監査人へアクセス権を付与することも可能。				
							1. AWS から入手できる情報、およびその他の必要な情報をレビューして IT 環境全体について可能な限り理解し、すべてのコンプライアンス要件を文書化します。				【参考文献、参照URL】 ○注 1 https://aws.amazon.com/jp/artifact/ https://aws.amazon.com/jp/artifact/getting-started/ https://aws.amazon.com/jp/artifact/faq/#Compliance_Reports 2 https://aws.amazon.com/jp/compliance/soc-faqs/			
							2. 企業のコンプライアンス要件を満たす統制目標を設計し、実装します。							
							3. 社外関係者が行う統制を特定し、文書化します。							
							4. すべての統制目標が満たされ、すべての主要な統制が設計され、その運用が有効かどうかを検証します。							
							AWSの法務関連の情報は以下のサイトをご参照ください。 https://aws.amazon.com/jp/legal/ また、契約、その他法務関連のお問い合わせについては担当営業までご連絡ください。 - AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです - AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます - AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます - AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです							
							AWS環境にデプロイしたインフラストラクチャの統制に関して 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。AWS 環境を利用している場合の監査の実施について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。また、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。				(統24 5 記載行を参照)			
							SOX法の監査について お客様が AWS クラウドで会計情報を処理する場合、AWS システムの一部を Sarbanes-Oxley (SOX) の要件の範囲に組み込むことについては、お客様の監査人が判断することになるでしょう。お客様の監査人は、SOX の適用可能性について独自に判断する必要があります。ほとんどの論理アクセス統制はお客様が管理するため、関連する基準に統制活動が適合しているかどうかは、お客様が判断されるのが最適です。SOX 監査人が AWS の物理的統制に関する詳細情報が必要とする場合は、SOC 1 Type II レポートを参照できます。AWS が提供する統制が詳細に記載されています。							
							お客様のデータセンター訪問 AWS のデータセンターは多数のお客様をホストしており、そうした様々なお客様が第三者による物理的なアクセスに曝れることになってしまいうため、お客様によるデータセンター訪問を許可しておりません。このようなデータセンターに関するお客様のニーズを満たすために、SOC 1 Type II レポートの取り組みの一つとして、独立し、資格を持つ監査人がそのような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第三者による検証によって、お客様は運用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ぶ第三者によるセキュリティ認証 AWS の第三者レポートに文書化されているように、AWS データセンターに対する第三者の検証によって、AWS がセキュリティ認証取得に必要なとなるルールを確立するためのセキュリティ対策を適切に実装していることが保証されます。コンプライアンスプログラムとその他の要件により、外部の監査人はメディアの準備のテスト、監視カメラの録画映像の確認、データセンターの入り口と通路の監視、電子アクセス制御デバイスのテスト、データセンターの機器の調査などを実施します。				(統24 5 記載行を参照)			
							ISO/IEC 27001 規格は、ISO/IEC 27002 規格のベストプラクティスガイダンスに従い、セキュリティ管理のベストプラクティスと包括的なセキュリティ統制を規定したセキュリティ管理規格です。この認証の基礎は、情報セキュリティ管理システム (ISMS) などの強固なセキュリティプログラムの開発と実装です。ISMS では、AWS がどのようにしてセキュリティを体系的で包括的な方法で体系的に管理するかを定義しています。このように広く認められている国際セキュリティ規格では、次のことが指定されています。 ・情報セキュリティリスクを体系的に評価し、脅威と脆弱性の影響を考慮する ・総合的な情報セキュリティ統制や他の形式的リスク管理を設計および実装し、企業およびアーキテクチャのセキュリティリスクに対処する ・包括的な管理プロセスを採用し、統制により情報セキュリティのニーズが継続的に満たされるようにする							
							AWS は ISO/IEC 27001、27017、27018 の各規格に準拠しているという認証を取得しています。これらの認証は、サードパーティの独立監査人によって実施されます。このように国際的に認められた規格および実施基準に準拠しているということは、AWS が組織のすべてのレベルで情報セキュリティに取り組んでいること、および AWS のセキュリティプログラムが業界の主要なベストプラクティスに従っていることの証です。最新、詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/iso-27001-faqs/							
							SOCレポート AWS System & Organization Control (SOC) レポートは、重要なコンプライアンス管理および目標を AWS がどのように達成したかを実証する、独立したサードパーティによる審査報告書です。このレポートの目的は、お客様とお客様の監査人が、オペレーションとコンプライアンスをサポートするよう確立された AWS 統制を簡単に把握できるようにすることです。3 種類の AWS SOC レポートがあります。				(統24 5 記載行を参照)			
							SOC 1：AWS の統制環境に関する説明、および AWS が定義した統制と目標の外部監査に関する説明 SOC 2：AWS の統制環境に関する説明と AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たす AWS 統制の外部監査に関する説明 SOC 3：AWS が AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たしていることを実証する公開レポート							
							SOC3レポートは以下のURLからダウンロード可能です。 https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf 最新、詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/soc-faqs							
							AWSの認証や監査レポートに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/programs/ AWSのデータセンターに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/data-center/data-centers/							

「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

標準番号	役割	対応の主体		AWSの対応状況	お客様が統制すべき内容	参考情報	補足情報
		AWS	お客様				
統24	6	-	○		<p>・以下の各項目は、リスクベースでお客様固有のクラウドサービスに関連する統制を考慮する際の情報として参照ください。</p> <p>AWS環境の監査、ガイドライン、リスクやコンプライアンスに関する最新および詳細情報は下記のサイトをご参照ください。監査人向けのトレーニングコースの初回やAWS環境における監査の考え方に関連する資料などを掲載しています。</p> <p>https://aws.amazon.com/jp/compliance/resources/</p> <p>AWS セキュリティ監査のガイドライン</p> <p>セキュリティ設定を定期的に監査し、現在のビジネスのニーズに対応していることを確認する必要があります。監査では、不要な IAM ユーザー、ロール、グループ、およびポリシーを削除し、ユーザーとソフトウェアに対して必要なアクセス権限だけを与えるようにすることができます。セキュリティのベストプラクティスを実践するために、AWS リソースを体系的に確認し、モニタリングするためのガイドラインを示します。</p> <p>いつセキュリティ監査を行うか監査のための一般的なガイドライン</p> <ul style="list-style-type: none">- AWS アカウントの認証情報の確認- IAM ユーザーの確認 IAM グループの確認- IAM ロールの確認- SAML および OpenID Connect (OIDC) 用 IAM プロバイダの確認モバイルアプリの確認- Amazon EC2 セキュリティ設定の認証態のサービスの AWS ポリシーの確認 AWS アカウントのアクティビティの監視- IAM ポリシーを確認するためのヒント詳細情報 <p>最新、詳細情報は下記のサイトを参照ください。</p> <p>https://docs.aws.amazon.com/ja_jp/general/latest/gr/aws-security-audit-guide.html</p> <p>AWS 監査人のラーニングパスは、AWS のプラットフォームを使用して内部オペレーションのコンプライアンスを実証する方法を学習したいと考えている、監査人、コンプライアンス、および法的なロールを持っている方向けに設計されています。</p> <p>最新、詳細情報は下記のサイトを参照ください。</p> <p>https://aws.amazon.com/jp/compliance/auditor-learning-path/</p>		-
統24	7	-	○		<p>・AWSとお客様は、責任共有モデルに基づきIT 環境を統制することになります。AWS 側の責任は、安全性の高い、統制されたプラットフォームでサービスを提供し、幅広いセキュリティ機能をユーザーに提供することです。お客様の責任は、用途に合わせて安全かつ統制された方法で IT 環境を構築することにあります。ITシステムのプロイ方法にかかわらず、お客様はこれまでどおり、IT 統制環境全体に対する適切な管理を維持していただく必要があります。主な実施内容として、関連資料を基にしたコンプライアンスの目標と要件の把握、その目標と要件を満たす統制環境の構築、組織のリスク許容度に基づいた必要となる妥当性の把握、統制環境の運用の有効性の検証などがあります。AWS クラウドへのデプロイにより、企業が各種の統制や検証方法を採用するにあたって選択の幅が広がります。お客様のコンプライアンスと管理が厳格な場合は、次のような基本的なアプローチも考慮可能です。このような方法でコンプライアンス管理にアプローチすることで、社内の統制環境をより理解することができます。また、実行すべき検証活動を明確にすることもできます。</p> <ol style="list-style-type: none">1. AWS から入手できる情報、およびその他の必要な情報をレビューして IT 環境全体について可能な限り理解し、すべてのコンプライアンス要件を文書化します。2. 企業のコンプライアンス要件を満たす統制目標を設計し、実装します。3. 社外関係者が行う統制を特定し、文書化します。4. すべての統制目標が満たされ、すべての主な統制が設計され、その運用が有効的かどうかを検証します。 <p>AWSの法務関連の情報は以下のサイトをご参照ください。</p> <p>https://aws.amazon.com/jp/legal/</p> <p>また、契約、その他法務関連のお問い合わせについては担当営業までご連絡ください。</p> <ul style="list-style-type: none">- AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです- AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます- AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます- AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです <p>AWS 環境にデプロイしたインフラストラクチャーの統制に関して</p> <p>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、接続ポイントや送値の統制を含め、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。AWS 環境を利用している場合の監査の実施については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。また、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。</p> <p>SOX法の監査について</p> <p>お客様が AWS クラウドで会計情報を処理する場合、AWS システムの一部を Sarbanes-Oxley (SOX) の要件の範囲に組み込むことについては、お客様の監査人が判断することになるでしょう。お客様の監査人は、SOX の適用可能性について独自に判断する必要があります。ほとんどの論理アクセス統制はお客様が管理するため、関連する基準に統制活動が適合しているかどうかは、お客様が判断されるのが最適です。SOX 監査人が AWS の物理的統制に関する詳細情報が必要とする場合は、SOC 1 Type II レポートを参照できます。AWS が提供する統制が詳細に記載されています。</p> <p>お客様のデータセンター訪問</p> <p>AWS のデータセンターは多数のお客様をホストしており、そうした様々なお客様が第三者による物理的なアクセスに曝されることになってしまいうため、お客様によるデータセンター訪問を許可していません。このようなデータセンターに関するお客様のニーズを満たすために、SOC 1 Type II レポートの取り組みの一つとして、独立し、資格を持つ監査人がそのような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第三者による検証によって、お客様は運用されている統制の効果について独立した観点を導くことができます。AWS と機密保持契約を結ん</p>		-

「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

「AWS FISCC安全計画基準対応リファレンス」からの引用					AWSの対応状況	お客様が統制すべき内容	参考情報	補足情報
標準番 号	役割	対応の主体						
		AWS	お客様					
						<p>第三者によるセキュリティ認証</p> <p>AWS の第三者レポートに文書化されているように、AWS データセンターに対する第三者の検証によって、AWS がセキュリティ認証取得に必要なルールを確立するためのセキュリティ対策を適切に実施していることが保証されます。コンプライアンスプログラムとその要件により、外部の監査人はメディアの産業のテスト、監視カメラの録画映像の確認、データセンターの入り口と通路の監視、電子アクセス制御デバイスのテスト、データセンターの機器の調査などを実施します。</p> <p>ISO/IEC 27001 規格は、ISO/IEC 27002 規格のベストプラクティスガイダンスに従い、セキュリティ管理のベストプラクティスと包括的なセキュリティ統制を規定したセキュリティ管理規格です。この認証の基礎は、情報セキュリティ管理システム (ISMS) などの強固なセキュリティプログラムの開発と実装です。ISMS では、AWS がどのようにしてセキュリティを全体で包括的な方法で体系的に管理するかを定義しています。このように広く認められている国際セキュリティ規格では、次のことが指定されています。</p> <p>-情報セキュリティリスクを体系的に評価し、脅威と脆弱性の影響を考慮する</p> <p>-総合的な情報セキュリティ統制や他の形式のリスク管理を設計および実装し、企業およびアーキテクチャのセキュリティリスクに対処する</p> <p>-包括的な管理プロセスを採用し、統制により情報セキュリティのニーズが継続的に満たされるようにする</p> <p>AWS は ISO/IEC 27001、27017、27018 の各規格に準拠しているという認証を取得しています。これらの認証は、サードパーティの独立監査人によって実施されます。このように国際的に認められた規格および実施基準に準拠しているということは、AWS が組織のすべてのレベルで情報セキュリティに取り組んでいること、および AWS のセキュリティプログラムが業界の主なベストプラクティスに従っていることの証拠です。最新、詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/iso-27001-faqs/</p> <p>SOCレポート</p> <p>AWS System & Organization Control (SOC) レポートは、重要なコンプライアンス管理および目標を AWS がどのように達成したかを実証する。独立したサードパーティによる審査報告書です。このレポートの目的は、お客様とお客様の監査人が、オペレーションとコンプライアンスをサポートするよう確立された AWS 統制を簡単に把握できるようにすることです。3 種類の AWS SOC レポートがあります。</p> <p>SOC 1：AWS の統制環境に関する説明、および AWS が定義した統制と目標の外部監査に関する説明</p> <p>SOC 2：AWS の統制環境に関する説明と AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たす AWS 統制の外部監査に関する説明</p> <p>SOC 3：AWS が AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たしていることを実証する公開レポート</p> <p>SOC3レポートは以下のURLからダウンロード可能です。 https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf 最新、詳細情報は下記のサイトを参照ください。 https://aws.amazon.com/jp/compliance/soc-faqs</p> <p>AWSの認証や監査レポートに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/programs/ AWSのデータセンターに関する 詳細情報は下記を参照ください。 https://aws.amazon.com/jp/compliance/data-center/data-centers/</p>		
統24	8	-	○	変更についての通知はAWSカスタマーアグリーメント(1.5,1.6)およびAWSのサービス条件(1.6)において以下の通り定めております。		<p>AWS Config は、設定が異な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 全体でチェックとカードレールのデプロイが自動化され、公開されたリソースを特定および修復します。</p>		<p>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</p> <p>AWSカスタマーアグリーメント https://aws.amazon.com/jp/agreement/</p> <p>AWSのサービス条件 https://aws.amazon.com/jp/service-terms/</p>
統25	-	-	○	-		-		-
統26	-	-	○	-		-		-
統27	-	-	○	-		-		-

「AWS FISCC安全対策実施事例対応フレームランス」からの引用					「対応の主体」凡例					
実施順	段階	対応の主体			参考情報	「AWS FISCC安全対策実施事例対応フレームランス」からの引用			参考情報	
		AWS	企業	その他		お客様が提供すべき内容	参考情報			
第1	-	-	○	-		お客様がAWS上で実施するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の情報を用いて、お客様にて実施します。	【概要】 ●監視番号、パスワード等、利用権・システム管理権が使う秘密文字列を安全に管理します。 ●システム管理については、システム管理者(人)に該当するIAMユーザに加え、コマンドラインツール、REST API等、人以外に該当するパスワード相当の秘密文字列があるため注意が必要です。 ●秘密文字列の例 ▲人が担当の場合：IAMユーザ、OS/ミドルウェアユーザ、アプリケーションユーザなど ▲プログラムが対象の場合：コマンドラインツールのアクセスキー・シークレットアクセスキー 【対策例】 ●IAMユーザや、アクセスキー・シークレットアクセスキーは、セキュリティディレクトリブランチ(*)に適切な設計する(後述URL参照)。 ●認証情報等、OS/ミドルウェアが使う認証情報はパラメータストアやSecrets Managerに格納する。 ●Webやモバイルアプリケーション認証・認可には、Amazon Cognitoの活用も検討する。 ●Cognitoユーザプールは、アプリケーションのサインアップ、サインイン、サインアウトなどユーザディレクトリを提供、MFA機能あり。 ●Cognito Federated ユーザーディレクトリは、SAMLやOpenID Connect対応の外部IDP(*)2と連携可能(SSO)。 (*)1本人認証のセキュリティと信頼を上げるために、多要素認証(MFA)の設定を実施する。 (*)2Google/Facebook/LinkedInのActive Directory等。 【参考文献、参照URL】 ・IAM のセキュリティディレクトリベストプラクティス https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html ・AWS Systems Manager Parameter Store https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-parameter-store.html ・AWS Secrets Manager https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/intro.html ・Amazon Cognito とは https://docs.aws.amazon.com/ja_jp/cognito/latest/developerguide/what-is-amazon-cognito.html	-		
第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 による 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・ルートユーザを使用している場合です。AWS に対してフェレシジョンを行うか、または他の方法により IAM ロールを割り当てる場合、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実行できます。	【第1 記載行を参照】	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 FISCC セキュリティの柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-	
						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、! @ # % ^ & * () _ + = [] ' の記号のうち、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(Account Settings(アカウント設定) ページで、AWS アカウントの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。	【第1 記載行を参照】			
						ID の使用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。				
第2	-	-	○	-		お客様がAWS上で実施するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の情報を用いて、お客様にて実施します。	【概要】 ●データへの適切なアクセス制御を行います。 ●無事(漏洩)の際にもデータの漏洩が最小限になるように、重要なデータは暗号化を行います。 【対策例】 ●アクセス制御 ●アクセスコントロールのための各種ポリシーを利用します。例えば、IAM ユーザなどデータにアクセスする際に設定する「アイデンティティベースのポリシー」や、S3のバケットポリシーやKMSのキーポリシーなど、アクセスされるデータ単位に設定する「リソースベースのポリシー」があります。 ●暗号化 ●EBS、RDS、EFS、S3等、各種ストレージに格納するデータは暗号化します。全般的に AWS KMSを使った暗号化が可能。 ●S3では、データ格納時の暗号化(クライアント側暗号化)と、格納アプリケーション側での暗号化、復号化の両方によるクライアントサイド暗号化を選択可能(暗号化暗号鍵の管理は別)。Secrets Manager(Parameter Store)の暗号化も検討(*)。 (*)1 AWS KMS よりも重要なキーの管理や、高いコンプライアンス要件がある場合は、AWS CloudHSMの利用も検討。 【参考文献、参照URL】 ●Amazon EC2 のデータ保護 https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/data-protection.html ●Amazon RDS リソースの暗号化 https://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/Overview.Encryption.html ●Amazon S3 のセキュリティディレクトリベストプラクティス(Amazon S3 のセキュリティディレクトリベストプラクティス) https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/security-best-practices.html#server-side-encryption ●EFS保管時のデータの暗号化 https://docs.aws.amazon.com/ja_jp/efs/latest/ug/encryption-at-rest.html	-		
第3	-	-	○	-		お客様がAWS上で実施するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の情報を用いて、お客様にて実施します。	【概要】 ●暗号化に用いられる乱数や秘密鍵を保護するためのサービスとして、AWS Key Management Service(KMS)を活用しています。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います (https://aws.amazon.com/iam/ 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IAWクラウドセキュリティポータルページ(https://aws.amazon.com/security/entry-point)を参照してください。AWS は、AWS インフラストラクチャ内で暗号化される必要な暗号化の暗号キーを内部で生成、管理、保持しています。AWS は、AWS 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する暗号暗号キーを生成、保持、配布しています。暗号キーの作成、保護、配布には、AWS が開発したセキュアおよび認証暗号マネージャーを使用し、必要と必要な AWS 認証情報、RSA プラットフォーム・ハードウェア、および X.509 認定セキュアプラットフォーム環境、保持するために使用されます。AWS は暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な監視のために、第三者の独立監査によって確認されます。	【第3 記載行を参照】		
第3	8	-	○			キーの保存、ローテーション、アクセス権限を含む暗号化プロセスを定義することで、不正ユーザーからのランソムの保護や、不正ユーザーへの不正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、多量の AWS 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、柔軟性と安全性が高く、冗長なストレージを使用できます。キーのエイリアスの追加、キーレベルのポリシーも定義できます。ポリシーは、キー管理やキーユーザを定義するの役に立ちます。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 クラウド上での独自の暗号化キーを完全に主として管理できます。FIPS 140-2 レベル 3 認証済みの HSM を使用することで、データセキュリティに関する企業、業界、規制のコンプライアンス要件を満たすことができます。	【第3 記載行を参照】		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	アイデンティティサービス：リスクエンジニアリング https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepaper/AWS_S_Risk_and_Compliance_Whitepaper.pdf
第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。暗号化に使用する生成済みデータキーは、256 ビット、128 ビット、または鍵長 1024 ビットまでの任意の長さ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。カスタム暗号のローテーションやプロパティの管理、追加が利用可能になることを管理します。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、データを暗号化するには必要ありません。AWS KMS は通常のバージョンのキーを自動的に保護して、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。	【第3 記載行を参照】	AWS KMS の暗号化の詳細情報 https://docs.aws.amazon.com/ja_jp/kms/latest/developerguide/encryption-primitives.html	AWS Well-Architected フレームワーク FSI Lens for FISCC 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-	
						https://docs.aws.amazon.com/ja_jp/iam/latest/developerguide/cryptographic-details/cryptographic-primitives.html				

「AWS FISCC安全対策基準対応リファレンス」からの引用					「AWS FISCC安全対策基準対応リファレンス」からの引用					「AWS FISCC安全対策基準対応リファレンス」からの引用				
実装順序	段階	対応の主体		AWSの対応状況	参考情報	対応策が適用すべき内容	参考情報	参考情報	対応策が適用すべき内容	参考情報	対応策が適用すべき内容	参考情報		
第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情報を用いて、お客様にて実施します。	<p>[概要]</p> <p>AWSの利用においてデータ伝送路に監禁された場合でもデータの内容がわからないようにするため、システム利用者がAWSマネジメントコンソールやAWS API、または開発したアプリケーションにアクセスする際の経路及び開発者/利用者による維持管理の経路を暗号化します。</p> <p>・データが漏洩した場合を考慮し、データ自体を暗号化します。</p> <p>[対策例]</p> <ul style="list-style-type: none">■AWSマネジメントコンソール及びAWS APIによる操作をする場合の伝送データの暗号化防止■伝送経路の暗号化<ul style="list-style-type: none">・AWSマネジメントコンソール及びAWS APIによる操作はデフォルト設定されているHTTPSによる暗号化通信を利用します。■アプリケーションへのアクセスする際の伝送データの暗号化防止<ul style="list-style-type: none">・HTTPSやSSH等の暗号化済みのプロトコルを使った通信や、VPNを利用した通信経路の暗号化が有効です。・専用線（Direct Connect）を利用した場合でも暗号化等の暗号化防止策は必要です。■伝送するデータの暗号化<ul style="list-style-type: none">・AWS Key Management Service (KMS) というキー管理サービスを使って、各サービス・各リソースの暗号化を行います。■AWSサービスの暗号化<ul style="list-style-type: none">・S3 や Application Load Balancer など、AWSサービス毎にデータ通信の暗号化についての考え方が変わります。 <p>特許や知的所有権の侵害を防止するための対応状況を確認し、利用の際には暗号化通信の実装が必要です。</p> <p>例：S3/バケットポリシーを利用して暗号化通信を強制する。Application Load Balancer でHTTPリクエストをHTTPSにリダイレクトする。</p> <p>[参考文献、参考URL]</p> <p>https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/encryption-in-transit.html</p> <p>https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/example-bucket-policies.html</p> <p>https://docs.aws.amazon.com/ja_jp/elasticbeanstalk/latest/dg/configuring-https-httpsredirect.html</p>	-						
第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。これを実現する厳格な方法として、AWS Certificate Manager (ACM) 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とだけでなく、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を ACM (Amazon EC2) インスタンス、コンテナなどを使用して提供できます。	<p>[概要]</p> <p>データ伝送時における重要なデータのデータ保護の対策について確認する</p> <p>[対策例]</p> <p>(1) 伝送経路上における暗号化の範囲</p> <p>以下項目については、データの伝送経路が暗号化されていることを前述の内容を基として確認します。</p> <ul style="list-style-type: none">■AWSマネジメントコンソール及びAWS APIによる操作をする場合の伝送データの暗号化防止■アプリケーションへのアクセスする際の伝送データの暗号化防止 <p>(2) クラウドサービスで提供される暗号化機能等</p> <p>データ伝送時における暗号化機能等の確認観点に対して、対策例を以下に記載します。</p> <ul style="list-style-type: none">・クラウドサービスで提供される暗号化の暗号化の方法<ul style="list-style-type: none">⇒AWS Certificate Managerの利用 (SSL/TLS証明書の管理)・クラウドサービスの伝送データの暗号化機能<ul style="list-style-type: none">⇒SSL/TLS証明書による通信暗号化⇒管理インフラフェーズへのアクセスにおけるHTTPS 通信のための証明書⇒左記に記載 <p>(第4 記載行を参照)</p>	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/sec_protect_data_transit_key_cert_mgmt.html									
						AWS のサービスには、通常は 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。コネクティングリソースを完全に解凍して、サービス全体に伝送中データの暗号化を実現できます。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 に電話する際、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。特許な要件がある場合は、AWS Marketplace でサードパーティ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									
第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情報を用いて、お客様にて実施します。	(第4 記載行を参照)	-						
第5	3	-	○	-		アクセス（最小特権を使用）、分離、バージョンングなど、複数のコントロールによって侵害中のデータを保護できます。データのアクセスは、AWS CloudTrail などの監査メカニズムと、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。	<p>[概要]</p> <p>AWSアカウント上で設定しているアクセス制御が、定義したセキュリティ基準から逸脱していないかを継続的・継続的に確認し、必要に応じて逸脱しうる設定を防止します。</p> <p>[対策例]</p> <p>1. AWS SecurityHubでセキュリティ基準・AWS Configルールを用いた設定の準拠状況の確認及び非準拠状態の自動検出</p> <ul style="list-style-type: none">・アクセス制御に係るAWS SecurityHubのセキュリティ基準のコントロールやAWS Configカスタムルールを有効化することで、AWSアカウント内のリソースのアクセス制御の状態を継続的・継続的に監視します。・コントロール・ルールに非準拠となる設定を検出した場合にアラート通知する仕組みを設定することで、非準拠設定を早急に検知し設定の修正を促します。・AWS Configルールで修復アクションを設定することで、満たすべきセキュリティ基準を逸脱した設定を検出した場合に、自動的に修復します。・ただし、AWS Configルールは、評価回数で費用が変動する課金体系上、費用が高騰する恐れがあるため注意が必要です。 <p>2. サービスコントロールポリシーを用いた不適切操作の防止</p> <ul style="list-style-type: none">・AWS Organizations全体、もしくは特定のAWSアカウント群に対して同一の予防的統制を施す場合にサービスコントロールポリシーを利用できます。・実際に使っていない操作をサービスコントロールポリシーで定義し、監視対象のAWSアカウントが所属するOUに適用することで、誤操作や悪意のある操作ができなくなります。・サービスコントロールポリシーは、メンバーアカウントのルートユーザの権限を制御することができます。・ただし、ポリシーの設定内容や通知頻度を誤ると、本来実施可能な操作が実施できなくなり、影響が広がる恐れがあるため、注意が必要です。	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/sec_protect_data_rest_access_control.html									
						AWS 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継続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、多段階のアクセス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。重要なファイアウォール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ー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 エンドポイントやブリックワ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。								
第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情報を用いて、お客様にて実施します。								
第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情報を用いて、お客様にて実施します。	<p>[概要]</p> <p>特定システムでオープンネットワークを介した利用者とAWS環境間の重要なデータ伝送には、改ざん検知の対策が必要となります。</p> <p>[対策例]</p> <ul style="list-style-type: none">■伝送データの改ざん検知の対策として、TLS通信の利用が挙げられます。Webサーバなどの前段に配置するAWSのサービスにおいてHTTPSを有効にすることで、TLSが導入されるメッセージ認証により、クライアントとサーバ間のデータの改ざん検知の対策を行うことができます。・AWSのサービスでは、TLSの利便性を高めるサービス(Elastic Load Balancing)と強制されるサービス(例: Amazon API Gateway)があり、前者を利用する場合に利便性と利便性の両立でTLSの導入を行う必要があります。Elastic Load Balancingなどに適用する証明書は、AWS Certificate Manager を使用して作成することができます。・WebサーバでTLS処理を行う構成では、TLSの処理負荷の軽減と秘文の保護を目的に、AWS CloudHSM を利用することができます。■AWS APIリクエストへの署名を機軸により、リクエストデータの改ざん検知を行うことができます。AWS APIリクエストを送信するカスタムプログラムを作成する場合は、リクエストに署名するコードを実装します。AWS CLI または AWS SDK を使用してAWS APIリクエストを作成する場合は、ツールの設定で既定したアクセスキーにより自動的に署名されます。■特定システムなど安全対策の水準を高める必要がある場合には、署名データの電子署名によるデータの改ざん検知の対策を検討します。アプリケーションの開発において AWS KMS API などを使用し、クライアントのアクセスキーにより署名データの電子署名を行い、伝送経路を通じたデータ(署名データを含む)の取り扱ひの後、サーバ側でデータの署名検証を行います。■Amazon S3 にデータをアップロードまたはダウンロードする際に、データの整合性検証の機能により、データ転送時の改ざん検知の対策を行うことができます。	-						

© 2023, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

「AWS F15C安全対策基準対応リファレンス」からの引用					「AWS F15C安全対策基準対応リファレンス」からの引用					「対応の主体」 凡例	
実装例	図表	形式の名称			参考情報	実装例が提供するサービス内容	参考情報		実装例が提供するサービス内容	：必要に応じて情報を提供する	
		AWS	拡張性							(AWS F15C安全対策基準対応リファレンス) からの引用	補足情報
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。	(参考文書、参照URL) (※ 1)AWS マネジメントコンソールのよくある質問 ・ウェブコンソール Q: セッションはいつ失効しますか? https://aws.amazon.com/jp/console/faq-console/ (※ 2)AWS Identity and Access Managementユーザーガイド ・Amazon EC2 インスタンスで実行するアプリケーションに対し、ロールを使用する ・ロールを使用してアクセス許可を委任する https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html (※ 3)AWS Identity and Access Managementユーザーガイド ・AWS での多要素認証 (MFA) の使用 https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_mfa.html ・AWS: 遠隔元 IP に基づいて AWS へのアクセスを拒否する https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/reference_policies_examples_aws_deny-ip.html (※ 4)Amazon Cognito デベロッパーガイド ・Amazon Cognito ユーザーグループに対するセキュリティのベストプラクティス https://docs.aws.amazon.com/ja_jp/cognito/latest/developerguide/managing-security.html (※ 5)AWS Identity and Access Managementユーザーガイド ・AWS アカウントのルートユーザーのベストプラクティス https://docs.aws.amazon.com/ja_jp/accounts/latest/reference/best-practices-root-user.html				
実10	-	-	○	-		お客様のAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実装します。	(概要) AWS利用に伴い、追加でアクセス権限の取得・保管・監査対象となるものとして、下記があります。 アクセス権限取得・保管・監査のための対策を検討・実装します。 ・AWSリソース自体の操作権限 ・AWS マネジメントコンソールへのアクセス権限 ・AWSリソースに対するアクセス権限 (例：Amazon S3・Amazon RDS等のデータへのアクセス権限、ELB・Amazon CloudFront・Amazon API Gateway・AWS AppSyncへのアクセス権限) (対策例) AWSリソース自体の操作権限を取得する手段としてAWS CloudTrailが提供されています。AWS CloudTrailによりAWSリソース操作時のAPIの実行履歴やマネジメントコンソールのアクセス履歴を出力・保管することができ、当該情報を監査記録として活用可能です。(※ 1) AWSリソースに対するアクセス権限は、各サービスで提供されているインテグレーションにより収集・保管可能です。 〔一部サービスの例数(※ 2)(※ 3)(※ 4)(※ 5)(※ 6)(※ 7)に示します。〕 なお、OS上でのレイヤで断すべき対策はオンプレミス環境利用時と考え方が変わるものではありません。 また、周知による不正アクセス行為の抑制についてはオンプレミス環境利用時と考え方が変わるものではありません。 (参考文書、参照URL) (※ 1)AWS CloudTrail ユーザーガイド ・AWS CloudTrail でのセキュリティのベストプラクティス https://docs.aws.amazon.com/ja_jp/awsccloudtrail/latest/userguide/best-practices-security.html (※ 2)Amazon Simple Storage Service ユーザーガイド ・AWS CloudTrail を使用した Amazon S3 API コールのログ記録 https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/cloudtrail-logging.html ・サーバーアクセスログを使用したリクエストのログ記録 https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/ServerLogs.html (※ 3)Amazon Relational Database Service ユーザーガイド ・Amazon RDS データベースログファイルの取得 https://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/USER_LogAccess.html (※ 4)Elastic Load Balancing Application Load Balancer ・Application Load Balancer を監視する https://docs.aws.amazon.com/ja_jp/elasticloadbalancing/latest/application/load-balancer-monitoring.html (※ 5)Amazon CloudFront開発者ガイド ・標準ログ (アクセスログ) の設定および使用 https://docs.aws.amazon.com/ja_jp/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html (※ 6)Amazon API Gateway開発者ガイド ・API Gateway での CloudWatch による REST API のログの設定 https://docs.aws.amazon.com/ja_jp/apigateway/latest/developerguide/set-up-logging.html (※ 7)AWS AppSyncデベロッパーガイド ・モニタリングとログ記録 https://docs.aws.amazon.com/ja_jp/appsync/latest/devguide/monitoring.html				
実10	8	-	○	-		マネジメントコンソールのアクセス権限はCloudTrailに記録されます。 https://docs.aws.amazon.com/ja_jp/awsccloudtrail/latest/userguide/cloudtrail-event-reference-aws-console-sign-in-events.html CloudTrail が記録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 が記録した期間のファイルを検証することができます。 https://docs.aws.amazon.com/ja_jp/awsccloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html	(概要) 実10の参考情報に記載の通りですが、AWS利用に伴い、AWS マネジメントコンソールのアクセス権限の取得・保管・監査が必要です。 (対策例) (1) アクセス権限の取得と保管期間 ログ生成時、ログイン失敗時の履歴、操作ログについては、AWS CloudTrailにて取得することが可能です。 CloudTrailから確認できる保管期間は90日であり、長期保存のためにはS3へ出力する等、設定が必要です。(※ 1) (2) アクセス権限の改ざん、不正アクセスに対する防止策 CloudTrailや侵害検出システム等に対するアクセス権限を適切に設定し、変更・削除の操作を実施できるユーザを限定する必要があります。 また、CloudTrailの整合性検証機能を活用することで、ログファイルの改ざん有無を確認できます。(※ 2) (3) アクセス権限の偽造防止・タイミング アクセス権限は取得・保管のみではなく、定期的な監査が必要です。 CloudTrailのログを確認するサービスとして、CloudTrail Lake等を活用することができます。(※ 3) (参考文書、参照URL) (※ 1)AWS CloudTrail ユーザーガイド ・CloudTrail の仕組み https://docs.aws.amazon.com/ja_jp/awsccloudtrail/latest/userguide/how-cloudtrail-works.html (※ 2)AWS CloudTrail ユーザーガイド ・CloudTrail のログファイルの整合性検証を有効にする https://docs.aws.amazon.com/ja_jp/awsccloudtrail/latest/userguide/cloudtrail-log-file-validation-enabling.html (※ 3)AWS CloudTrail ユーザーガイド ・イベントデータストアを作成する https://docs.aws.amazon.com/ja_jp/awsccloudtrail/latest/userguide/query-event-data-store.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

【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

「AWS FISCC安全対策標準対応リファレンス」からの引用					「AWS FISCC安全対策標準対応リファレンス」からの引用					「AWS FISCC安全対策標準対応リファレンス」からの引用				
実装例	図表	形式の主体	AWSの対応状況		参考情報	お客様が確認すべき内容					参考情報	補足		
実10	9	-	○	-		CloudTrail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 サービスにも利用されます。このサービスは、各 AWS リージョンで複製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 に追加されたうる秒を自動的に同一化します。 https://docs.aws.amazon.com/ja_jp/AWSSEC2/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 時刻を使用します。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_for					(実10 記載行を参照)			
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、ログファイルが複製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 を活用することもできます。Amazon S3 /バケットオブジェクトのライフサイクルポリシーを有効にし、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履歴データを使用して、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) が常態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 のリソースの保護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履歴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10 記載行を参照)	AWS Well-Architected フレームワーク FSI Lens for FISCC セキュリティの注 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上で実施するシステムおよびサービスの管理は、AWSが提供する機能および情報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上で実施するシステムおよびサービスの管理は、AWSが提供する機能および情報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	-	-	○	-	[概要] AWSは、暗号化に用いられる共通鍵や秘密鍵を保護するためのサービスとして、AWS Key Management Service (KMS) を提供しています。AWS KMSを用いることで、暗号化キーを安全に管理し、適切な権限を持つIAMユーザーまたはアプリケーション(AWSにおいて、アプリケーションと特称されます)に対してのみ、その暗号化キーの利用を制御することになります。これらのサービスの提供により、AWSは取り扱うデータに関する暗号化およびアクセス制御などのデータの保護に係る認証を取得しています。金融機関等は、自らの責任において、暗号鍵を適切に保護して管理することすることができま	お客様がAWS上で実施するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。					[概要] ●暗号鍵を安全に管理します。 [詳細] ●要件に応じ、下記サービスを検討 (暗号鍵利用における監査ログはAWS CloudTrailにより自動取得される)。AWS CloudHSMは、AWS社にも暗号鍵へのアクセスをさせない、FIPS140-2のような厳しい基準事項が必要といった、高いコンプライアンス対応のためのサービス。但し、いずれのケースにおいても、顧客要件が満たせるかの確認は必要。 ●AWS Key Management Service (暗号鍵は、ユーザ管理 or AWS管理のいずれかを選択) ●AWS CloudHSM ●キーポリシーの設定 (暗号鍵へのアクセス制限、詳細は参考文献)。必要に応じ、IAMポリシー (使用) でのアクセス制御を設定する事も可能(*1)。 ●(オプション) 暗号鍵の自動ローテーションを設定。 (*1)キーポリシー、IAMポリシーの両方を設定した場合、両方で許可された操作のみ可能。 [参考文献、参照URL] ●AWS Key Management Service とは https://docs.aws.amazon.com/ja_jp/kms/latest/developerguide/overview.html ●AWS KMS でのキーポリシーの使用 https://docs.aws.amazon.com/ja_jp/kms/latest/developerguide/key-policies.html ●AWS CloudHSM とは https://docs.aws.amazon.com/ja_jp/cloudhsm/latest/userguide/introduction.html		-	
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、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ポライバーバー(http://aws.amazon.com/security (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提供される重要な暗号化用の暗号キーを外部に提供、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組み合わせて、暗号化キーを作成、管理、配布しています。対象キーの作成、保護、配布は、AWS が開発したセキュアキーおよび認証情報 暗号化キーが使用され、ホストに必要な AWS 認証情報、RSA /ハッシュアルゴリズム、および X.509 認定をセキュアポリシー 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。	[関連する認証] ●ISO/IEC 27001 ●PCI DSS ●要件3.5 カード会員データを保護と使用から保護するために使用される鍵を保護するための手順を文書化し、実施する ●要件3.6 カード会員データの暗号化に使用される暗号化鍵の管理プロセスおよび手順をすべて文書化し、実施する。 [参考文献、参照URL] ●AWS Key Management Service のよくある質問 https://aws.amazon.com/jp/kms/faq/	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 で暗号化する手法です。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することはできません。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するための推奨されます。カスタマー管理の CMK は、キーの寿命や使用にわたる柔軟性を提供します。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 を用いて記録されます。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md	(実13 記載行を参照)	AWS Well-Architected フレームワーク FSI Lens for FISCC セキュリティの注 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、暗号化を行う秘鍵の管理側とデータを所有するリソースの管理者を分離することに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 でカスタマーマスター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変更することが可能になります。例えば、故意/過失に陥らず Amazon S3 内のオブジェクトを不正な非許可インテグリティに公開してしまった場合でも、暗号化を行う秘鍵側のキーポリシーでインターネットから秘鍵へのアクセスが許可されていないければ、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13 記載行を参照)	AWS Well-Architected フレームワーク FSI Lens for FISCC セキュリティの注 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fsi-lens-for-fisc/security.md		

「AWS FISCC安全対策基準対応リファレンス」からの引用					「AWS FISCC安全対策基準対応リファレンス」からの引用		「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 「AWS FISCC安全対策基準対応リファレンス」からの引用	
基準番号	性質	対応の主体	対応の主体	対応の主体	参考情報	お客様が検討すべき内容	参考情報	対応の主体
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高度な保護機能を備えており、お客様はさらに重要な保護を実施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取ることができます。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、最も一般的で頻発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）およびアプリケーションの脆弱性の攻撃を統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新しい脅威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。 侵害または潜在的なモニタリングシステムから得られる情報の信頼性を分析し、必要に応じてセキュリティを強化します。リスクを表現して評価した後、Amazon は、不正行為者の特徴に符合する変更の使用状況が現れて	お客様がAWS上で実行するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の情報を用いて、お客様に実施します。 インフラストラクチャ保護: Amazon Virtual Private Cloud (Amazon VPC) を使用して、お客様が定義された仮想ネットワーク内で AWS リソースを開始できます。Amazon CloudFront は、DDoS を軽減する AWS Shield と統合されたビジネスに対して、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や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。	(実14 記載を参照)	Amazon Web Services: 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 への事例 https://d1.awsstatic.com/whitepapers/ja_jp/compliance/NIST_Cybersecurity_Framework_CSF.pdf
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 ウェブアプリケーションのルールセット (ウェブ ACL) に含まれるルールを変更する、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、業界をリードする同様の製品を提供しています。これらの製品は、既存の AWS サービスを使用し、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リソース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流量に関する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) にバッチリッシュできます。フローログを作成した後、選択した送信元でデータを取得したり表示したりできます。VPC トラフィックのモニタリングを検討する: トラフィックモニタリングは、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、コンパイル検査、機械学習、トラブルシューティングのために機械側セキュリティおよびモニタリングアプリケーションに連携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-	(図解) AWSのセキュリティサービスのログを継続的に分析することで、影響範囲や原因の特定を効率化します。 [図解] ・ログの継続的な分析には、Amazon Detectiveが活用できます。 ・Amazon Detectiveを利用する前段階として、分析手順、手法のマニュアル化や利用者の自発的な事前準備を行うことで、影響範囲や原因の特定の更なる効率化が期待できます。	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軽減するために、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 インスタンスにインストールすることで、AWS 上で実行されている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 を利用してログを AWS S3 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、監査ログが有効です。 手動されるネットワークトラフィックと手動しないネットワークトラフィックを監視します。不慣れたアクセスやネットワークトラフィックを監視します。例えば、ネットワークのメトリクスを監視し、異常時にも多量なトラフィックが検知される場合は攻撃を受けいる可能性があります。予見しない外部システムへの接続の試みは、外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監視します。 GuardDuty を使用して悪意のある外部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 を使用し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いて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 フラッシュ攻撃やアプリケーション攻撃といったレイヤー 3 とレイヤー 4 に対する攻撃のワークロードを守ります。AWS Shield Advanced 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-	(図解) AWS WAFには、AWS WAFのルールで定義された条件に一致したもののウェブリクエストの処理方法が複数あります。 [図解] ・初期のリクエストのバッチを確認するために、リクエストのCountだけリクエストは通過させる [Count] アクションを利用して、リクエストの情報を監視します。続いて、不慣れたリクエストのバッチが閾値を突破、リクエストを遮断する [Block] アクションに移行します。 ・このように段階的にバッチを実行することで、正確なリクエストを迅速なリクエストが検知されます。	AWS Well-Architected フレームワーク FSI Lens for FISCC セキュリティの柱 https://github.com/aws-	
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社の情報を掲載しています。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。	Amazon GuardDuty の Malware Protection の機能は、内部対策として、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスおよびコンテナワークロードのマルウェアの検知に役立ちます。また、下記の点に注意が必要です。 ・マルウェアが検知されるタイミングは、マルウェアに感染したAmazon Elastic Compute Cloud (Amazon EC2) インスタンス等が外部と通信し、その通信がAmazon GuardDutyによって検出されるタイミングです。よって、マルウェアと外部の通信が発生するまでは、感染に気づくことは困難です。 Amazon GuardDutyが行うのはマルウェアの検知のみであり、マルウェアの実行を止めることはできません。 上述した制約を鑑み、必要に応じてサードパーティのマルウェア対策ソフトウェアの導入をご検討ください。		
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14 記載を参照)		
実15	-	○	○	-	AWSネットワーク管理は、SOC、PCI DSS、ISO 27001、およびFedRAMPへのAWSの継続的な保護の一環として、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重要な情報を保護しています。また、特定のシステム設計を保持しているすべてのポートとプロトコルを監視しています。AWSは、デバイスの使用に不可欠な機能の最小実装という原則に基づいています。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、定期的な外部からの脆弱性スキャンが実行されます。脆弱性スキャンと解決手法は、AWSのPCI DSSおよびFedRAMPへの継続的な保護の一環として定期的に確認されます。 AWS PrivateLink を使用して、VPC と AWS のサービスをセキュアでスク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、サービスは直接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。	お客様がAWS上で実行するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の情報を用いて、お客様に実施します。 お客様がAmazon VPCを使用することにより、Amazon Web Services (AWS) クラウド内で論理的に分離されたクッ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 リソースを開始できます。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通信および発着のネットワークトラフィックを定義することができます。事前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、各サブネットに入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ク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、サービスは直接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。	(図解) ・外部ネットワークからのアクセス経路は最小限にします。 [図解] ・外部からAWS管理レイヤー(マネジメントコンソール及びAPI等)へのアクセス制御 ・IAMポリシーによる制御 ・アクセス元のIPアドレスを制御するIAMポリシーを、IAMユーザーやIAMロールに適用します。 ・IPアドレス制御により、特定のIPアドレス範囲からの通信を不要なネットワークアプリケーションから遮断します。 ・外部からの各リソースへのアクセス制御 ・AWSの機能で制御 ・セキュリティグループ等でIPおよびポート許可設定を行うことができます。 ・VPCのネットワークアクセスコントロールリストにて、アクセスできるIPアドレスの設定を行うことができます。 ・VPCエンドポイントを利用することにより、インターネットを経由せずAWSサービスへの接続できるようにより、外部にさらす部分を減らすことも有効です。 ・VPCの外に接続するリソース(代表例: S3/ウェブ)に対し、リソースベースのポリシーによって外部ネットワークからのアクセスを制御することができます。 ・AWS WAF が利用可能なAWSサービス(代表例: CloudFront)の場合は、AWS WAF で定義されたIPアドレス制御が可能です。 ・利用者の設定によって、特定のIPアドレス範囲に限定しない従来の制御 ・IPアドレスの範囲において、IPアドレスのアクセス制御の設定を行います。 ・アクセス元のIPアドレスを制御するIAMポリシーを、IAMユーザーやIAMロールに適用します。 ・AWS Systems Manager の Session Manager を利用することで、外部からアクセスするコンソールポートを開通することが可能です。 [参考文献、参考URL] https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/session-manager.html	Amazon Web Services: リスクとコンプライアンス

「AWS FISC完全対策基準対応リファレンス」からの引用					「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		
実装順序	段階	形式の名称	AWSの対応状況	参考情報	「AWS FISC完全対策基準対応リファレンス」からの引用	参考情報	
AWSの対応状況				お客様が提供するべき内容		確認情報	
実15	3	-	○	-	システムへの接続許可を、正当な理由やネットワークを利用して接続する場合のみにも与えるよう構成することで、特種多数の悪意からの不正アクセスを防止します。接続元の接続元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条件群を使用して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/fai-lens-for-fisc/security.md	【概要】 アクセス経路について提供方式毎に接続元IPアドレスを制御できることを確認する 【対策例】 ・基本型に管理インターフェースへのアクセスは、IAMポリシーで指定で接続元IPアドレス制御を行う。 ・AWSコンソールによっては、接続元IPアドレスが制御できないワークスがある。 ・利用するAWSサービスが接続元IPアドレスを制御できるが、事前に確認を行うこと。	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/fai-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ーを識別しています。サービスチームは監査機能を設定して、要件に合った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ことが発生すると自動的に調査を開始します。スクラッパ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、要求時に調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、監査記録が失敗した場合に、自動化されたアラートを受け取ります。監査記録の失敗には、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監視します。 AWS のコアおよびモニタリングプロセスは、SOC、PCI DSS、ISO/IEC 27001、および FedRAMPコンプライアンスへのAWSの継続的な監視のために、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 で実行のアプリケーションを継続すると、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機械学習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 ログで検出され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継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、悪意の検出、機械学習などの統合された機械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。	【概要】 ■不正アクセスを監視します(例えば、AWSコンソールへの不正アクセス、ルートユーザーの使用、IAMアクセスキーの大量利用、DDoS攻撃の誘発にされている等)。 【対策例】 ■Amazon GuardDuty(*)を有効にする。全リジョンでの有効化が推奨。 ■リアルタイム検知が必要であれば、CloudWatch Eventsと利用し、通知を実施。 ■その他、不正アクセス監視ツールとして、IDS(不正侵入検知システム)、IPS(不正侵入防御システム)、CASB(Cloud Access Security Broker)等を検討。 (*)Amazon GuardDutyは、CloudTrailログ、VPC Flow Logs、DNS Logsの情報に基づき、機械学習により様々な脅威を検出するサービス。 Amazon GuardDutyはこれらデータソースから抽出したデータストリームを直接取得するため、CloudTrailログ、VPC Flow Logs、DNS Logsは有料だけでなく無料の機能(後述、よる必要経路無し)で、よる必要経路無し。併し、これらのログは、有償のクラウドプラットフォームや、監視に利用されるため、有効化の上、適切な保存が必要となるケースが大部分、例)CloudTrailの有効化と、接続ログの保存・保護等。 【参考文庫、参考URL】 ■Amazon GuardDuty? 継続したセキュリティ監視と脅威の検知 https://aws.amazon.com/jp/blogs/news/amazon-guardduty-continuous-security-monitoring-threat-detection/ ■Amazon GuardDuty に関するよくある質問 https://aws.amazon.com/jp/guardduty/faqs/ ■[AWS Black Belt Online Seminar] Amazon GuardDuty 資料及び QA公開「IDSに変わるものではない?簡易使ったほうが良いものでしょうか?」 https://aws.amazon.com/jp/blogs/news/webinar-bb-guardduty-2018/	アマゾン ウェブ サービス：リスクとコンプライアンス
実16	2	-	○	-	Amazon GuardDutyなどのツールを使用して、疑わしい活動や変更された境界外にデータが移動させようとする試みを自動的に検知します。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に拡張し、ネットワークフローログ情報をチャプチャするAmazon VPC フローログをAmazon EventBridge などに転送して、異変を検知(検知は事前の許可)の機能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ものに役立ちます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/sec_protect_data_transit_data_unintended_access.html	(実16 記帳行を参照)	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。	-	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-
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きき鳴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、は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。リスクを発生して評価した後、Amazon は、不正行為の検知に符合する反復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開始に行えます。	【概要】 不正アクセスについては(1)アカウントに対する不正アクセスと、(2)AWS上のシステムに対する不正アクセス、それぞれのレイヤーで対策が必要ですが、また、不正アクセスの検知を確保し、インシデント発生後に迅速な対応と被害範囲の調査が出来るよう準備する必要があります。また、マルチアカウント利用時にはログの分散や取り忘れ、不要アカウントの消し忘れに起因する不正アクセスを防止するため、(3)マルチアカウント利用時の検知対策についても下記記載します。 【対策例】 1) AWSアカウントへの不正アクセス 不正アクセスがあった際の証跡確保と、調査が可能な状態とします。 ・ CloudTrail、GuardDuty、AWS Config、Amazon Detectiveの有効化 ・ AWS Security Hubを有効化し、検知結果とコンプライアンス事象状況の可視化を行う ・ 接続ログ保管用アカウントを分離し、侵入者が改ざん出来ない場所にログ保管する 復旧に際しては速いしたAWSアカウントキーの検知と、無効化を行います。 ・ Trusted Advisorを利用し、公開されたアクセスキーの検知と削除を行う。 ・ 接続ログを確認し、改ざん懸念の特定を行い、必要に応じてバックアップから復旧する。 再発防止対策は下記の通りです。 ・ MFA利用の徹底 ・ 長期に渡り利用可能なアクセスキーの利用を避け、IAMロールによる一時的なセキュリティ認証情報を使用する。 ・ Amazon Detectiveによる脅威調査と、GuardDutyおよびによる脅威検知 2) AWS上のシステムに対する不正アクセス OSの特定のアクセスを監視されるケースにおいては権限管理の徹底と、アクセス経路の特定、操作ログの取得が有効です。 ・ 権限管理システムを導入することでOSへの特権アクセス権限を一元的に管理、利用するたびに申請、承認ID/パスワードを払い出す体制とする。 ・ メンテナンスにはSystems Manager Session Managerを利用し、アクセス経路と監視ログの取得する。 ・ 踏み台環境を用意し、アクセス経路を限定する(ex. Security Group)による遠隔元IPの限定、Session Managerの利用 ・ 踏み台環境上でのターミナル操作ログの取得と、ログ証跡管理(接続ログ保管用アカウントを分離し、侵入者が改ざん出来ない場所にログ保管する) 公開しているアプリケーションに関してはユーザから接続システムまでのアクセス経路に置くゲートウェイ(他のセキュリティ装置)サービスとOSにインストールするホスト型セキュリティソフトウェアを組み合わせた、記録の確保と、悪意あるアクセスの進行の遅延を行う仕組みを用意します。 ・ AWS WAF、もしくはサードパーティのSaaS型WAFサービスの実装 ・ AWS Shield (Standard/Advanced)の実装によるDDoS対策 AWS内の脅威検知におけるポイント ・ Route3のクエリログの取得 ・ VPCフローログの取得 ・ ELBログの取得 ・ Webサーバーログの取得(ELBログの場合はhttpヘッダのx-forwarding-for項目の取得) ・ サーバ上にインストールするホスト型IDS/IPSによるログ取得 ・ AWS Network Firewall、もしくはサードパーティソフトウェアによるIDS/IPSの実装 ・ AWS Advanced改ざん検知ソフトウェアの導入 不正アクセスの検知と調査、分析のために上記ログの保全と、EBS Snapshot機能を利用したバックアップの作成を行います。 AWS上の設定/リソースをエクスポートするためのスクリプトを予め準備し、各AWSコンポーネントの設定値を取得して下さい。	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との関係 https://dl.awsstatic.com/whitepapers/ja_jp/compliance/NIST_Cybersecurity_Framework_CSF.pdf

實情基準

© 2023, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

「AWS FISCC安全対策基準対応リファレンス」からの引用					「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 「AWS FISCC安全対策基準対応リファレンス」からの引用		
実装例	対策	対応の主体	AWSの対応状況	参考情報	参考情報	対応の主体	
実25	-	○	○	AWS は、ISO/IEC 27001 に準拠して、AWS リソースに対する監理アクセスについて最小権限の標準を示す正規のポリシー、手続きを策定しています。AWS SOC レポートには、AWS リソースに対するアクセスロジシ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完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、リソース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渡されたレスポンス票など、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/ja/iam/	【概要】 コンピュータシステムの運用上もしくは業務上重要なファイルやデータを、アクセス権限所有が最小限となるよう制御する必要があります。 【対策】 AWSにてアクセス権限を制御する方法として下記が考えられます。 (1)アイデンティティベースのポリシー(IAM) IAMを利用して、個人・グループ・AWSリソースから業務上重要なファイルを保存しているAWSリソースへのアクセスを制御できます。 (2)リソースベースのポリシー AWSリソースにポリシーを適用することにより、AWSリソース内でアクセスを制御できます。 リソースベースのポリシーを利用できるAWSサービスは限定されます。 (3)AWS KMS(AWS Key Management Service) AWS KMSのカスタマー管理キーを利用することにより、IAMユーザー/IAMロール単位でのアクセス制御が可能となります。 不正アクセスが行われた場合のアクセス記録の取得に関する情報は【実10】を参照してください。 【参考文献、参照URL】 (1) IAM と連携する AWS のサービス https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/reference_aws-services-that-work-with-iam.html	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完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、リソース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渡されたレスポンス票など、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/ja/iam/	【概要】 AWSリソースへのアクセスをコントロールし、ログを取ります。 また、権限を定期的に監査し、不必要な権限を削除することが重要です。 【対策】 ・クラウド事業者が提供するアクセス権限の管理 AWSリソースへのアクセスは前述（実25 参見なし）の参考情報参照してください。 AWSリソースへのアクションのログを取得するにはCloudTrailを利用します。CloudTrailに関する情報は【実10】の参考情報参照してください。 ・アクセス権限を設定するための管理インターフェースへのアクセス 【実1】を参照してください。 ・外部事業者が提供するアクセス権限の設定のためのツール等を導入する場合の条件や制約 外部のアクセス権限を設定するツールを導入する場合は、当該ツールへのアクセスにAWSの管理インターフェースと同様のセキュリティを実装する必要があります。また、当該ツールに付与する権限も最小限にするよう配慮する必要があります。	PCI DSS 8.2.3 PCI DSS 8.2.4
実26	-	○	○	AWSではISO/IEC 27001およびPCI DSSに準じ、AWSリソースへの信頼的なアクセスのために必要なパスワードポリシーを策定しています。パスワードは複雑である必要があり、90 日おきに更新されます。 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II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 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完全にコントロールすることができます。AWS IAMでは、パスワードの動作を変更したり、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。自動パスワード失敗の抑制、以前に使用したパスワードの再使用禁止、次の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	【概要】 AWS上の各種資産やシステムへのアクセス権限の管理について、手続きを明確に定める必要があります。手続きについてはオンプレミスと同等の考えとなりますが、AWS特有のアクセス権限の管理について考慮する必要があります。 【対策】 AWSアカウント/IAMユーザー・ロール/アクセスキーの管理 AWSアカウントのルートユーザーは厳密に保護し、AWSリソースへのアクセスには最小権限のIAMユーザー・ロールを用い、各ユーザーに個別の資格情報を付与する。またのAWSアカウントを管理する場合は、AWS Organizations(AWS Service Control Policy)を利用を検討する。また、アクセスキーは定期的なローテーションし、不要なアクセスキーは削除する。 一時的な資格情報の利便性 一時的な資格情報サービスには、STS (Security Token Service) を使用して一時的な資格情報を発行する。 アクセス権限の定期的な監査 IAM Access Analyzer or CSPM などのツールを使用して、定期的にアクセス権限をレビューし、不要な権限を削除する。 【参考文献、参照URL】 ・AWS Well-Architected フレームワーク セキュリティの柱 - 権限管理 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/permissions-management.html ・AWS アカウントのルートユーザーへのベストプラクティス https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/root-user-best-practices.html#r-tp-secure ・AWS Organizations の概要 https://docs.aws.amazon.com/ja_jp/organizations/latest/userguide/orgs_introduction.html ・IAM の一時的な認証情報 https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_temp.html ・AWS Identity and Access Management Access Analyzer の使用 https://docs.aws.amazon.com/IAM/latest/UserGuide/what-is-access-analyzer.html	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、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要としています。承認しない、リソースへのアクセスは自動的に失われます。ユーザーアクセス権の承認の原則については、SOC2レポートに既述が記載されています。ユーザー権限の承認の原則については、SOC2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、ドメイン名及びアプリケーションのアクセス制御 認定事業者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たい。 認定事業者の更新がAmazonの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。従業員は権限に変更が生じる場合、リソースに対するアクセス権限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、ドメイン名及びアプリケーションの更新、ISO 27001認定事業者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たい。	【概要】 AWS のアクセス権限の管理は、ISO/IEC 27001 に準拠しています。AWS のアクセス権限の管理については、ISO/IEC 27001 の付録AおよびAWS SOC2レポートを参照してください。 【関連する認証】 -ISO/IEC 27001 -9.2 利用アクセスの管理 -9.4 システム及びアプリケーションのアクセス制御 【参考文献、参照URL】 ・AWS コンプライアンスプログラム https://aws.amazon.com/compliance/programs/	【概要】 AWS上の各種資産やシステムへのアクセス権限の管理について、手続きを明確に定める必要があります。手続きについてはオンプレミスと同等の考えとなりますが、AWS特有のアクセス権限の管理について考慮する必要があります。 【対策】 AWSアカウント/IAMユーザー・ロール/アクセスキーの管理 AWSアカウントのルートユーザーは厳密に保護し、AWSリソースへのアクセスには最小権限のIAMユーザー・ロールを用い、各ユーザーに個別の資格情報を付与する。またのAWSアカウントを管理する場合は、AWS Organizations(AWS Service Control Policy)を利用を検討する。また、アクセスキーは定期的なローテーションし、不要なアクセスキーは削除する。 一時的な資格情報の利便性 一時的な資格情報サービスには、STS (Security Token Service) を使用して一時的な資格情報を発行する。 アクセス権限の定期的な監査 IAM Access Analyzer or CSPM などのツールを使用して、定期的にアクセス権限をレビューし、不要な権限を削除する。 【参考文献、参照URL】 ・AWS Well-Architected フレームワーク セキュリティの柱 - 権限管理 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/permissions-management.html ・AWS アカウントのルートユーザーへのベストプラクティス https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/root-user-best-practices.html#r-tp-secure ・AWS Organizations の概要 https://docs.aws.amazon.com/ja_jp/organizations/latest/userguide/orgs_introduction.html ・IAM の一時的な認証情報 https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_temp.html ・AWS Identity and Access Management Access Analyzer の使用 https://docs.aws.amazon.com/IAM/latest/UserGuide/what-is-access-analyzer.html	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、検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承認は、グループ所有権が作成、確認されます。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、再割り当てされません。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90日間有効に承認されます。同時に、すべてのグループメンバーは必要に応じて、グループメンバーシップを失った後、自動的にシステムによって自動的に削除されます。この原則は、AWS アカウント管理ツールによってグループ所有権に関連したシステム通知によって開始されます。この通知では、グループのメンバーシップを失ったグループ所有権に伝えます。メンバーは、グループ所有権によるアクセス権限の完全な再評価です。メンバーがグループから失われた場合、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 日アクティブでなければならずシステムによって自動的に削除されます。AWS は AWS システムでシステム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、事件に就く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コースが発生すると自動的に容量を増やします。スワールで許可可能なサービスを提供するように設計されています。AWS API は更新可能な、SOC、PCI DSS、ISO 27001、およびFedRAMP AWS の継続的な更新のために、サービスバー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/バージョン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。データへのフルアクセスが与えら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業務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管理 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管理により、エンティティは、アイデンティティベースのポリシーとアクセス許可の権限の両方を管理しているアクションのみを実行できます。また、権限の拒否を防ぐために、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。アクセス権限は定期的に見直しが必要ですが、それ以外にも、所属や組織の変更に伴う権限の更新、入社や退職、休職、異動の発生、システムの退却やリタイア後のタスクの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らず、サービス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必要なアクセス権限付与の確認や、AWS IAM Access Analyzer による監視/不許可アクセス許可の確認が可能です。 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fis-lens-for-fisc/security.md	【実27 記載を参照】	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_r_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 FIS Lens for FISCC セキュリティの柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/blob/main/doc/fis-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。 AWSでは、顧客が適切な手段によってデータをさらに保護することを推奨します。	【概要】 データファイルの不正使用、改ざん、紛失等を防止するため、データファイルの複製・管理方法を明確にする必要があります。 お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 AWSでは、顧客が適切な手段によってデータをさらに保護することを推奨します。 【対策】 データは、お客様にてその重要度に応じた保存期間等、保管方法、保管場所を明確にする必要があります。 AWSでは、EBS ポリシーとSnapショットとをAES-256 で暗号化する機能があり、EC2 インスタンスをホストするサーバで暗号化が行われるため、EC2 インスタンスと EBS ストレージとの間を移動するデータを暗号化できます。 Amazon S3 では、保管時のデータの暗号化利用に複数のオプションを用意しており、暗号化プロセスの管理を行いたい場合は、Amazon S3 のサーバーサイド暗号化(SSE)を使用できます。Amazon S3 の SSE により、オブジェクトを書き込む際に追加のクイックスタートを参照に追加するだけで、アップロード時にデータを暗号化することもできます。データの暗号化は、自動的に暗号化が行われます。ただ、オブジェクトに含めることができるメタデータは暗号化されないため、Amazon S3 メタデータに暗号化情報を含めないことをお勧めします。	-

「AWS FISCC安全対策基準事例対応リファレンス」からの引用						「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	
記事番号	掲載	対応の主体		AWSの対応状況	参考情報	「AWS FISCC安全対策基準事例対応リファレンス」からの引用	参考情報	
		企業	AWS	お客様		お客様が提供するべき内容	顧客情報	
第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。	-	
第30	-	-	○	-	<p>[概要]</p> <p>■AWSは、暗号鍵を管理するためのサービスとして、Amazon KMS や、AWS CloudHSM を提供しており、その仕様は、AWS の Web サイト上で公開されています。金融機関等が AWS の機能を利用して暗号鍵を管理する場合、満足した手続きを実現するための機能は AWS 上に存在するかを確かめる必要があります。</p> <p>[関連する認証]</p> <p>■ISO/IEC 27001</p> <p>●10.1 番号による管理策</p> <p>■PCI DSS</p> <p>●要件3.5 カード会員データを暗号化と照用から保護するために使用されるキーを保護するための手順を文書化し、実施する。</p> <p>●要件3.6 カード会員データの暗号化に使用されるキーの管理プロセスおよび手順をすべて文書化し、実施する。</p>	<p>お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。</p>	(第30 記載行を参照)	-
第30	4	-	○	-		<p>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。数値的に選ば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長さにすることができます。AWS KMS ではお客様の呼び出しに 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 (AES-GCM) が使用されます。カスタマ-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も選択した場合は、データを暗号化する必要はありません。AWS KMS は高可用性のバージョンのキーを自動的に保持し、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。</p> <p>https://docs.aws.amazon.com/ja_jp/kms/latest/cryptographic-details/crypto-primitives.html</p>	<p>[概要]</p> <p>■AWS Key Management Service (AWS KMS) および AWS CloudHSM では、FISCC安全対策基準で述べられている「鍵管理に対する認証とアクセスの制限」において、以下の機能を有しています。利用者は、これらの機能を利用して、みずから生成した暗号鍵を適切に管理する必要があります。</p> <p>●KMS キーのキーポリシーによるアクセス制御 (*1)</p> <p>●KMS キーのIAMポリシーによるアクセス制御 (*2)</p> <p>●CloudHSM キーストアでのIAMポリシーによるアクセス制御 (*3)</p> <p>■AWS Key Management Service (AWS KMS) および AWS CloudHSM では、FISCC安全対策基準で述べられている「金融機関等がみずから生成した暗号鍵を使用する場合」において、以下の機能を利用しています。利用者は、これらの機能を利用して、みずから生成した暗号鍵を適切に管理する必要があります。</p> <p>●KMS キーのキーメディアのインポート機能 (*4) ●CloudHSM の キーのインポート機能 (*5)</p> <p>[参考文献、参考URL]</p> <p>■(*1) AWS KMS のキーポリシー</p> <p>https://docs.aws.amazon.com/ja_jp/kms/latest/developerguide/key-policies.html</p> <p>■(*2) AWS KMS で IAM ポリシーを使用する</p> <p>https://docs.aws.amazon.com/ja_jp/kms/latest/developerguide/iam-policies.html</p> <p>■(*3) AWS CloudHSM キーストアへのアクセスの制限</p> <p>https://docs.aws.amazon.com/ja_jp/kms/latest/developerguide/authorize-key-store.html</p> <p>■(*4) AWS KMS キーのキーメディアのインポート</p> <p>https://docs.aws.amazon.com/ja_jp/kms/latest/developerguide/importing-keys.html</p> <p>■(*5) AWS CloudHSM の キーのインポート</p> <p>https://docs.aws.amazon.com/ja_jp/cloudhsm/latest/userguide/import-keys.html</p>	<p>AWS KMS の暗号化の詳細説明</p> <p>https://docs.aws.amazon.com/ja_jp/kms/latest/cryptographic-details.html</p> <p>■AWS Well-Architected フレームワーク FSI Lens for FISCC セキュリティの注</p> <p>https://github.com/aws-samples/baseline-environment-aws-for-financial-services-institute/blob/main/doc/fai-lens-for-fisc/security.md</p>
第31	-	○	○	○	新たに採用した従業員には体系的な入社研修を行い、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。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	(第31 記載行を参照)	アパレン ウェブ サービス：リスクとコンプライアンス
第31	4	-	○	○		<p>「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掲載する優れた方法です。</p> <p>https://aws.amazon.com/jp/news/</p> <p>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、個人を支え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状態で、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タデータが存在します。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。</p> <p>https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/ops_evolve_ops_knowledge_management.html</p> <p>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、組織全体のメモリを豊かする必要があります。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。</p> <p>https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/ops_evolve_ops_knowledge_management.html</p>	<p>[概要]</p> <p>・クラウドサービス超過のシステム変更が頻繁に発生することが考えられるため、留意します。</p> <p>[対策例]</p> <p>クラウドサービス超過のシステム変更に関する注意点を整理します。</p> <p>・AWS マネジメントコンソールは頻繁に変更されるため、画面構成に影響を受けないマニュアルを作成する</p> <p>・リリース情報 (AWS の最新情報など) の内容を確認し、が発行されたらマニュアルへの影響を確認する変更点を確認する</p> <p>・マニュアルに影響がある場合、マニュアルを改訂変更し、必要に応じて教育訓練を実施する</p> <p>上記のほか、システム変更によるマニュアルへの影響程度を下げる手法として、Infrastructure as Code を活用した手動オペレーションの削減などが挙げられます。</p>	<p>AWS Well-Architected フレームワーク 運用上の優秀性の注</p> <p>https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/welcome.html</p> <p>AWS の最新情報</p> <p>https://aws.amazon.com/jp/news/</p>
第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。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	[概要] <p>お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。</p> <p>ウイルス対策に関しては、オンプレミスと同等に導入された技術的防衛対策の管理・保守の手続きを明確にする必要があります。</p> <p>加えて通知・報告手順については金融機関の責任範囲内でのセキュリティイベントとインシデント対応手順として整備する必要があります。</p> <p>クラウド特有の考慮として、金融機関責任範囲内で発生したインシデント対応については、ネットワーク内での感染拡大やフォレンジック調査等のための手段の確保を考慮したクラウド事業者との情報連携手順について必要に応じて明確化します。</p> <p>また、クラウド事業者責任範囲内で発生したインシデントに関する情報連携手順に関しても同様となります。</p> <p>[参考文献、参考URL]</p> <p>■AWS セキュリティインシデント対応ガイド</p> <p>お客様が AWS クラウド環境におけるセキュリティインシデント対応の場面に必要に応じて閲覧を提供します。クラウドセキュリティとインシデント対応の概念に注目し、お客様がセキュリティ機能に必要に応じて利用できるクラウド内の機能、サービス、メタデータについて説明します。</p> <p>https://docs.aws.amazon.com/ja_jp/whitepapers/latest/aws-security-incident-response-guide/welcome.html</p>	アパレン ウェブ サービス：リスクとコンプライアンス
第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。	-	

【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

「AWS FISCC安全対策基準対応リファレンス」からの引用				「AWS FISCC安全対策基準対応リファレンス」からの引用		「AWS FISCC安全対策基準対応リファレンス」からの引用	
記事番号	注釈	対応の主体	AWSの対応状況	参考情報	お客様が提供するべき内容	参考情報	対応の主体
第34	-	○	○				
AWS ネットワーク管理は、SOC、PCI DSS、ISO/IEC 27001、および FedRAMP 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 アドレスに依存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）。判別した脆弱性があれば、修正するために適切な手順に通知します。さらに、脆弱性に対する外部からの脅威の度合い、独立したセキュリティ会社によって定期的に実行されます。これらの意図に起因する発見や脆弱性は、分類整理されて AWS 上層部に報告されます。さらに、AWS 脆弱性は、通常の定期的および外部の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 の脆弱性発見と外部を確認およびテストしています。AWS セキュリティ戦略は、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べき標準アラームと告発メカニズムに基づいて、AWS のモニタリングチーム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信頼性を分析し、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、不正行為の脅威に符合する実質的な使用状況が現れているアカウントを無効にします。							
第34	4	○	-				
AWS セキュリティは、サービスエンドポイント IP アドレスに依存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）。判別した脆弱性があれば、修正するために適切な手順に通知します。さらに、脆弱性に対する外部からの脅威の度合い、独立したセキュリティ会社によって定期的に実行されます。これらの意図に起因する発見や脆弱性は、分類整理されて AWS 上層部に報告されます。さらに、AWS 脆弱性は、基礎となる AWS インフラストラクチャの健全性と可用性を確認するためのものであり、顧客固有のコンプライアンス要件に適合する必要がある。顧客自身の脆弱性スキャンに置き換わることを意味するものではありません。お客様は事前に承認を得た上で、お使いのクラウドインフラストラクチャにスキャンを実行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 利用規約に準拠しない場合があります。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、 AWS のセキュリティとプライバシーのガイドライン を参照してください。							
第35	-	○	○				
AWS では AWS 4 年間のシステムオペレーティングワークフロープロセスの一端として、一部のユーザー 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 を確保し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メーカーの承認が求められます。最初の認証は、デバイスプロビジョニングプロセスの一部としてユーザーに提供と提供されることととも、デバイスにも提供されます。その後、ユーザーは SSO パブリックキーをアカウントに追加することができます。システムアカウントの認証は、リクエストの ID を確認した後で、アカウント作成プロセスの一部としてリクエストに提供されます。							
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物理的手段を用いる専門の保安要員の他の手段により、厳密に管理されています。権限を付与されたスタッフか 2 要員認証を必要とすることで、データセンターの入り口にアクセスします。							
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 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。							
第35	2	-	○				

【AWS FISCC安全対策標準対応リファレンス】からの引用					【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			
記事番号	掲載	対応の主体	AWSの対応状況	参考情報	お客様が確認すべき内容	参考情報		
第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通知、検知、検証、承認、デプロイ、レポート、監査するための枠組みが十分に機能しています。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、記録、監査されているかが詳しく記載されています。	お客様がAWS上で実施するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	【概要】 オプレシスと関連し、検証されたオペレーションが指示どおり処理されたことを確認できるようにAWSオペレーションの記録を残すことが必要です。 【詳細】 第37の対策事項を参照		
第39	-	-	○	-	【概要】 AWS のバックアップは、ISO/IEC 27001 に準拠しています。AWS のバックアップについては、ISO/IEC 27001 の付録 A およびAWS SOCレポートを参照してください。なお、AWS カスタマーアグリーメントにおいて、サービス利用者が定期的にサービス利用権コンテンツを保存するために適切な手段をとることが求められています。データのバックアップは、責任共有モデルに基づき、利用権自身で適切な管理を行うことが必要となります。 【関連する認証】 ・ISO/IEC 27001 ・12.3 バックアップ 【参考文献、参照URL】 ・AWS カスタマーアグリーメント https://aws.amazon.com/jp/agreement/	お客様がAWS上で実施するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 【概要】 データファイル層書き及び災害等への対応のため、コンティジェンシープランと整合性のとれた適切な保管期間・保管サイズ・保管場所でのバックアップを取得するとともに、バックアップデータの管理を行うことが必要となります。そのために、AWSの責任で取得するバックアップの範囲及びAWSが提供するバックアップ機能を確認し、その活用を検討することが必要です。 【詳細】 お客様が実施するシステムの範囲において、バックアップを取得・管理する方法として下記が考えられます。 ・AWS Backup によりバックアップスケジュール、ライフサイクル管理を自動化して適切にバックアップを取得する。 ・EC2/EBSのバックアップについては、Amazon Data Lifecycle Manager の利用を検討する。 ・重要なバックアップについては、AWS Backup のクロスリージョンバックアップ機能を利用して、リージョンを異にしてバックアップを納貯する。なお、日本国外へのクロスリージョンにおいては、個人情報等の機密情報の取り扱いに関して国内・国外の法令・ガイドライン等に留意する必要がある。 ・バックアップデータは、必要に応じて暗号化するとともに、アクセスポリシーを定義しデータの操作リスクを低減する。 また、バックアップデータの安全管理においては、セキュリティ・対策等・利用権(保管データの取り出しに要する期間)、コストについて考慮する必要がある。AWSでは、費用対効果に優れたバックアップの保管場所として、AWS S3、S3 Glacier、S3 Glacier Deep Archiveといったサービスを活用することができます。その他の対策については、AWSはFISCC安全対策標準対応リファレンスおよびAWS各サービスのドキュメントを参照してください。 【参考文献、参照URL】 ・AWS Backup https://docs.aws.amazon.com/ja_jp/aws-backup/latest/devguide/whatbackup.html ・Amazon Data Lifecycle Manager https://docs.aws.amazon.com/ja_jp/AWSSEC/latest/UserGuide/snapshot-lifecycle.html ・個人情報保護法に関する法律についてのガイドライン (外国にある第三者への提供) https://www.ppc.go.jp/personalinfo/legal/guidelines_offshore/ ・Amazon S3 ストレージクラス https://aws.amazon.com/jp/s3/storage-classes/?nc=swliboc=3	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/whitepaper/rja_jp/compliance/NIST_Cybersecurity_Framework_CSF.pdf	
第39	5	-	○	-	【第39 記載行を参照】	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 分間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も備えています。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、クラウド、またはクラウドリージョンから継続的なデータ保護を保持できます。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 マネージドデータストア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。このデータは AWS で保管するには、Amazon S3 バックアップを使用できます。 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削減します。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、プライマリリカバリの場合はデータ復元が可能です。 このようセリ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 を使用する場合、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。バックアップ機能を提供するだけでなく、データの復旧にかかる時間を減らすことも、データの復旧に必要な時間、バックアップのタイプ (バックアップ範囲の場合) やデータ再生成メカニズムの複雑性に依存します。この場合は、ワークロードの RTO 以内でなければなりません。 【参考文献、参照URL】 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/welcome.html	【第39 記載行を参照】	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
第40	-	-	○	-		お客様がAWS上で実施するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-	
第41	-	-	○	-		お客様がAWS上で実施するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-	
第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。変更の実行段階への投入は通常、最も影響の小さいリソースの段階的なテストであり、影響が軽微であるよう確認してモニタリングされます。AWS変更管理プロセスでは、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.変更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.影響別に分類された非運用環境に変更をテストします。 4.ビジネスへの影響と範囲と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.帰属のある者による変更の承認を得ます。 【参考文献、参照URL】 ■AWS System & Organization Control (SOC) レポート AWS System & Organization Control (SOC) レポートは、重要なコンプライアンス管理および目標を AWS がどのように満たしたかを証明する、独立したサードパーティによる外部監査報告です。このレポートの目的は、お客様とお客様の監査人が、オペレーションとコンプライアンスをサポートするよう確立された AWS 統制と標準に照準を定めることです。3 種類の AWS SOC レポートがあります。 https://aws.amazon.com/jp/compliance/soc-faq/	【概要】 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。変更の実行段階への投入は通常、最も影響の小さいリソースの段階的なテストであり、影響が軽微であるよう確認してモニタリングされます。AWS変更管理プロセスでは、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.変更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.影響別に分類された非運用環境に変更をテストします。 4.ビジネスへの影響と範囲と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.帰属のある者による変更の承認を得ます。 【参考文献、参照URL】 ■AWS System & Organization Control (SOC) レポート AWS System & Organization Control (SOC) レポートは、重要なコンプライアンス管理および目標を AWS がどのように満たしたかを証明する、独立したサードパーティによる外部監査報告です。このレポートの目的は、お客様とお客様の監査人が、オペレーションとコンプライアンスをサポートするよう確立された AWS 統制と標準に照準を定めることです。3 種類の AWS SOC レポートがあります。 https://aws.amazon.com/jp/compliance/soc-faq/	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サービスであり、ご利用のAWS リソースのイベントリ、構成変更、構成変更の機能を提供します。AWS Config 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 リソースイベントのエクスポートが可能になり、特定の構成でどのようなリソースが構成されたかを可視化します。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。 【参考文献、参照URL】 ■OPS05-BP03 構成管理システムを使用する 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、変更を導入するのを助けます。 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/ops_dev_integ_conf_mgmt_sys.html ■AWS Config AWS Config は、AWS、オンプレミス、その他のクラウド上のリソースの設定と関係を継続的に評価、監査、評価します。 https://aws.amazon.com/jp/config/	AWS CSA Consensus Assessments Initiative Questionnaire (CAIQ)	
第42	1	-	○	-	【第42 記載行を参照】	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、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 AppConfig を使用して、アカウント全体のリソース全体の 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、構成変更の追跡、構成変化の他のリソースへの影響、AWS Config Rules および AWS Config コンフォーマンツクを使用して検出される、または望まれる設定との比較監査を行えます。 【ドキュメント、参照URL】 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/ops_dev_integ_conf_mgmt_sys.html	【概要】 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、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、アカウント全体のリソース全体の 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、構成変更の追跡、構成変化の他のリソースへの影響、AWS Config Rules および AWS Config コンフォーマンツクを使用して検出される、または望まれる設定との比較監査を行えます。 【参考文献、参照URL】 ■AWS Config AWS Config は、AWS、オンプレミス、その他のクラウド上のリソースの設定と関係を継続的に評価、監査、評価します。 https://aws.amazon.com/jp/config/	AWS Well-Architected フレームワーク 運用と信頼性の柱 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/welcome.html
第42	4	-	○	-	【第42 記載行を参照】	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/awsccloudtrail/latest/userguide/cloudtrail-event-reference-aws-console-sign-in-events.html	【概要】 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。 【参考文献、参照URL】 ■AWS Identity and Access Management AWS Identity and Access Management (IAM) を使用すると、AWS のサービスとリソースにアクセスできるユーザーやグループを指定し、きめ細かなアクセス許可を一元管理し、アクセスを分析して AWS 全体でアクセス許可を改善することができます。 ■AWS Cloud Trail AWS CloudTrail は、AWS インフラストラクチャ全体のアカウントアクティビティをモニタリングして記録し、ストレージ、分析、および構造化アクションをコントロールできます。 https://aws.amazon.com/jp/cloudtrail/	

【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

「AWS FISCC安全対策基準対応リファレンス」からの引用					「AWS FISCC安全対策基準対応リファレンス」からの引用					「AWS FISCC安全対策基準対応リファレンス」からの引用				
実装例	注釈	対応の主体			参考情報	対応の主体	注釈	対応の主体	注釈	参考情報	対応の主体	注釈	対応の主体	
		AWS	お客様	その他										
実42	参考	-	○	○	AWSの対応状況	環境保護デバイスは、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制御する専用保護デバイス（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承認、承認後、定期的に（少なくとも 24 時間ごと）情報保護デバイスに自動的にアップロードされ、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。	[実42 記載行を参照]			お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の情報を用いて、お客様にて実装します。	[概要] AWS上のネットワーク情報の構成管理。不正変更の検知についてはAWS Configが利用が有効です。リソースの承認とドメイン承認を指定した場合は、設定許可と、バリエーションの承認後書も合わせて実装します。設定情報を含むファイルのバックアップについては実装段階の内容を参照下さい。なお、AWS管理下のネットワークおよびそのインフラストラクチャの運用、セキュリティについてはAWSクラウドセキュリティに関するWebページ、クラウドサービスプロバイダーのセキュリティに関する調査資料を参照	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_r.pdf		
実43	-	○	○	○	AWSのバックアップおよび復元メカニズムは、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復元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。	[概要] AWSのバックアップは、ISO/IEC 27001に準拠しています。AWSのバックアップについては、ISO/IEC 27001の付録AおよびAWS SOC2レポートを参照してください。なお、AWS カスタマーアグリーメントにおいて、サービス利用権を定期的にサービス利用権コンテンツを保存するために適切な手段をとることが求められています。データのバックアップは、責任共有モデルに基づき、利用者自身で適切な管理を行うことが必要となります。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の情報を用いて、お客様にて実装します。	[概要] AWS上のネットワーク情報の構成管理。不正変更の検知についてはAWS Configが利用が有効です。リソースの承認とドメイン承認を指定した場合は、設定許可と、バリエーションの承認後書も合わせて実装します。設定情報を含むファイルのバックアップについては実装段階の内容を参照下さい。なお、AWS管理下のネットワークおよびそのインフラストラクチャの運用、セキュリティについてはAWSクラウドセキュリティに関するWebページ、クラウドサービスプロバイダーのセキュリティに関する調査資料を参照	アマゾン ウェブ サービス：リスクとコンプライアンス					
					[関連する記述] ・ISO/IEC 27001 ・12.3 バックアップ [参考文献、参照URL] ・AWS カスタマーアグリーメント https://aws.amazon.com/jp/agreement/				[対策例] 1) AWS Configの構成管理機能の利用 2) ネットワーク構成、設計、設定（ランチャーグループの管理） 3) AWS CLIによる設定情報を監視、保管（AWS Configでサポートされていないサービスの場合） 4) 設定ファイル、構成図ファイルの保存先としてEFS、S3を利用し、遠隔地バックアップを有効にする（実39参照） [参考文献、参照URL] ・AWS Config ベストプラクティス https://aws.amazon.com/jp/blogs/news/aws-config-best-practices/ ・AWSクラウドセキュリティに関するWebページ https://aws.amazon.com/jp/security/ ・クラウドサービスプロバイダーのセキュリティに関する調査資料(英文:Amazon Web Services CSA Consensus Assessments Initiative Questionnaire (CAIQ) IVS-08.1) https://d1.awsstatic.com/whitepapers/compliance/CSA_Consensus_Assessments_Initiative_Questionnaire.pdf					
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網羅的に確認し、重要なイベントや変更に基づいて更新します。定期的なモニタリングは、主要なビジネスメトリクスが稼働しなくなり、ビジネスの優先順位が変化した場合に、メトリックがワークロードに異常に反応できるようにします。モニタリングを監視することで、アプリケーションがどのタイミングで可用性の問題を発生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把握できるサービスを提供しています。Amazon CloudWatch Logs: このサービスはログを保存してその検索を支援します。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: さまざまな時点でのAWSインフラストラクチャが使用されているかを監視できます。AWS CloudTrail: このAWS APIが、いつ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レビューと知識の共有を定期的にを行うことで、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。	[実43 記載行を参照]	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、お客様の設計と信頼性の維持を最も重視していた。可用性、完全性、機密性の観点からAWS製品の品質管理を定義します。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システムを含む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情報を用いて、お客様にて実装します。	https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-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					
実45	-	○	○	○	AWSのインシデント対応プログラム、計画、および手順は、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機関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（ホウワットページ）」（ 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情報を用いて、お客様にて実装します。		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、外部の開発者の使用において、様々なオンラインツールを用いた積極的なモニタリングが可能です。AWS内のシステムには様々な装置が備わっており、主要なオペレーティングシステムをモニタリングしています。重要計測値が正常値から外れ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。オンコールスタッフが採用されているので、担当者が運用上の問題について対応できます。 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を構成メカニズムに基づいて、AWSのモニタリングアラームからセキュリティ情報または疑念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情報を用いて、お客様にて実装します。	Amazon CloudWatchは、AWSのクラウド資源及びお客様が使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。	[概要] システムの異常状態や不正使用を発見するための監視体制の整備は必須で、AWSのセキュリティ関連サービスを利用した異常や不正の検知とセキュリティ状況を一元的に可視化するための監視体制の整備が可能である。 [対策例] ■システムの異常状態の検知 ・Amazon CloudWatchアラームを利用し、AWSのサービスのメトリクスが事前設定のしきい値を超えたときに異常検知し、事前に決められた方法で担当者にアラーム通知します。 ■システムの監視機能 ・Amazon GuardDutyを利用し、AWS環境で発生するAWSアカウントやリソースに対する不正使用などの脅威を検知することができます。 ■セキュリティ状況の一元的可視化 ・AWS Security Hubを利用し、AWS環境のセキュリティ対応上層やコンプライアンスの遵守状況を一元的に可視化することができます。 ■対応すべき脅威の調査 ・Amazon Detectiveを利用し、AWS CloudTrailやAmazon GuardDutyなどのAWSサービスの情報を入力とし、セキュリティ問題の根本原因を分析・調査することができます。 ■監視とモニタリングの活用 ・Amazon CloudWatch Syntheticsを利用し、エンドポイントの可用性やレイテンシーなどをチェックし、実際のユーザーよりも早くシステムの問題を検出するためのユーザー体験の監視（Synthetic Monitoring）を行うことができます。 ■分散アプリケーションの分析とデバッグ ・AWS X-Rayを利用し、アプリケーションやその基盤となるサービスの実行状況を監視してパフォーマンスの問題やエラーの根本原因を特定するための調査を行うことができます。	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					

【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

「AWS F15C安全対策基準対応リファレンス」からの引用					「AWS F15C安全対策基準対応リファレンス」からの引用					「AWS F15C安全対策基準対応リファレンス」からの引用																																																																					
図表番号	図表	形式の名称	形式のバージョン	形式の更新履歴	参考情報	参考情報	参考情報	参考情報	参考情報	参考情報	参考情報	参考情報	参考情報	参考情報	参考情報	参考情報	参考情報	参考情報	参考情報																																																												
図46	2	-	○	-	AWSの対応状況					AWSの対応状況					AWSの対応状況					AWSの対応状況																																																											
					AWSの対応状況					AWSの対応状況					AWSの対応状況					AWSの対応状況																																																											
<p>ログファイルとメトリクスの照会を収集し、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役立ちます。</p> <p>Amazon CloudWatch Logs には、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 によってデータをクエリしたりできるクエリ言語もサポートされています。</p> <p>豊富な種類のフォーマットでのクエリがサポートされています。詳細 サポートされる Service とデータの形式、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 クラスタを実行してペタバイト規模の分析を実行できます。</p> <p>検知、診断、分析、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コストに固有です。モニタリングプロセスで関連とされがちな点は、データ管理です。モニタリングのためのデータ管理要件を決定し、それに合っ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 Lifecycle へのライフサイクル管理をサポートしています。</p> <p>このライフサイクル管理には、バケット内の（スゴ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、保存期間の終了後は期間切れにすることができます。S3 Intelligent-Tiering ストレージクラスは、パフォーマンスの改善と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頻度に基づ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。</p> <p>https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/monitor_aws_resources_storage_analytics.html</p>																				<p>お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。</p> <p>AWS Cloudwatchは、AWSのクラウド資源およびお客様が適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。</p> <p>また、AWS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。</p>																				<p>【図表】</p> <p>■各種資源の使用状況、健全性を監視します。</p> <p>【対策例】</p> <p>■メトリクス、ログ、 イベント情報の可視化サービスであるCloudWatchを利用する。デフォルトで収集される情報(メトリクス等)が不足する場合は、各種エージェントを追加設定するなど検討を行う。</p> <p>■アプリケーション監視など(APM)、より詳細な情報が必要な場合は、監視SaaSや、OSS、サードパーティ製ツール等の導入も検討します。</p> <p>■AWS全体のサービス健康状態はService Health Dashboardで確認しつづ、利用するアカウントごとに影響を確認する場合はAWS Health Dashboardを利用します。</p> <p>■不正検出サービスとして、Amazon GuardDuty、AWS Security Hub、Amazon Inspector、Amazon Detective、AWS Config、AWS Trusted Advisor等が利用可能です。</p> <p>【参考文献、参照URL】</p> <p>■AWS Health Dashboard (Service Health) https://status.aws.amazon.com/ ■AWS Health Dashboard - アカウントヘルスについて始める - AWS Health</p>																				<p>AWS Webサイト：AWSのコントロール・セキア対策</p> <p>https://aws.amazon.com/jp/compliance/data-center/control/</p>																			
図47	3	-	○	-	AWSの対応状況					AWSの対応状況					AWSの対応状況					AWSの対応状況																																																											
					AWSの対応状況					AWSの対応状況					AWSの対応状況					AWSの対応状況																																																											
<p>AWS モニタリングツールは、複雑な、または不正なアクティビティと事件を通知の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、ポートスキャンやアクティビティ、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組みをモニタリングします。このツールを使用して、複雑なアクティビティに対して検知に性能低下基準のしきい値を設定することができます。</p> <p>AWS 内のシステムには膨大な数のログが蓄積されており、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異常を示し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。</p>																				<p>お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。</p> <p>AWS Cost Explorerで特定期間の相対度を有効にし、AWS Cost and Usage Report (CUR)を作成します。これらのデータソースは、相対度およびコストと相関性をもとに分析します。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相対度、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 など限定可能なすべてのディメンションがあります。</p> <p>https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/cost-optimization-pillar/cost_monitor_usage_detailed_source.html</p> <p>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ために役立つ AWS のサービスです。クォータ値が既定値に達して、Service Quotas コンソールから、または AWS SDK を使用してクォータ増額のリクエスト、承認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）。スロットアウトされたAPIのエンドポイント増額など、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。</p> <p>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、プロビジョント IDPS、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 アドレスの増額を管理するために役立つ機能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、緩和論の権利についてお問い合わせください。</p>																				<p>【図表】</p> <p>・AWSのサービスやテナント側のサービスについて、構成、サポート期間、バージョン管理を行います。</p> <p>【対策例】</p> <p>■AWSサービスの構成管理</p> <p>・利用するAWSサービスのうちバージョンが存在しているサービスについてはEOSLの確認、有効期間が存在するサービスについては、有効期間の満期を行うことが必要です。</p> <p>■修正情報、不具合情報、パッチ情報を収集し、対応を検討することもあります。</p> <p>・取得方法として、公式ドキュメントの確認、メール配信するなどの設定を行うことができサービスがあります。</p> <p>■テナント側の構成管理</p> <p>・利用するOS以上のサービスについて、製品入手可能期間とサポート期間の確認を行うことが必要です。</p> <p>・利用するOS以上のサービスについて、修正情報、不具合情報、パッチ情報を収集し対応を検討することも必要です。</p>																				<p>AWS Well-Architected フレームワーク 信頼性の柱</p> <p>https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/welcome.html</p> <p>AWS Well-Architected フレームワーク コスト最適化の柱</p> <p>https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/cost-optimization-pillar/welcome.html</p>																			
図47	4	-	○	-	AWSの対応状況					AWSの対応状況					AWSの対応状況					AWSの対応状況																																																											
					AWSの対応状況					AWSの対応状況					AWSの対応状況					AWSの対応状況																																																											
<p>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（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ップ（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（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ップ（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最適化サーモスタットのように機能し、既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。</p> <p>https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/adapt_to_changes_proactive_adapt_auto.html</p>																				<p>【図表】</p> <p>・AWSのサービスやテナント側のサービスについて、構成、サポート期間、バージョン管理を行います。</p> <p>【対策例】</p> <p>■AWSサービスの構成管理</p> <p>・利用するAWSサービスのうちバージョンが存在しているサービスについてはEOSLの確認、有効期間が存在するサービスについては、有効期間の満期を行うことが必要です。</p> <p>■修正情報、不具合情報、パッチ情報を収集し、対応を検討することもあります。</p> <p>・取得方法として、公式ドキュメントの確認、メール配信するなどの設定を行うことができサービスがあります。</p> <p>■テナント側の構成管理</p> <p>・利用するOS以上のサービスについて、製品入手可能期間とサポート期間の確認を行うことが必要です。</p> <p>・利用するOS以上のサービスについて、修正情報、不具合情報、パッチ情報を収集し対応を検討することも必要です。</p>																				<p>AWS Well-Architected フレームワーク 信頼性の柱</p> <p>https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/welcome.html</p>																																							
図48	-	○	○	-	AWSの対応状況					AWSの対応状況					AWSの対応状況					AWSの対応状況																																																											
					AWSの対応状況					AWSの対応状況					AWSの対応状況					AWSの対応状況																																																											
<p>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ハイパーウェアの両面に所有権を割り当て、追跡および監視を行っています。AWSの調整およびサブプライチエンチームは、すべてのAWSサブプライチエンチームと関係を持っています。</p> <p>追加の詳細については、ISO/IEC 27001:2005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。</p>																				<p>お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。</p> <p>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管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識別し、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制御できます。</p>																				<p>【図表】</p> <p>・AWSのサービスやテナント側のサービスについて、構成、サポート期間、バージョン管理を行います。</p> <p>【対策例】</p> <p>■AWSサービスの構成管理</p> <p>・利用するAWSサービスのうちバージョンが存在しているサービスについてはEOSLの確認、有効期間が存在するサービスについては、有効期間の満期を行うことが必要です。</p> <p>■修正情報、不具合情報、パッチ情報を収集し、対応を検討することもあります。</p> <p>・取得方法として、公式ドキュメントの確認、メール配信するなどの設定を行うことができサービスがあります。</p> <p>■テナント側の構成管理</p> <p>・利用するOS以上のサービスについて、製品入手可能期間とサポート期間の確認を行うことが必要です。</p> <p>・利用するOS以上のサービスについて、修正情報、不具合情報、パッチ情報を収集し対応を検討することも必要です。</p>																				<p>アマゾン ウェブ サービス：リスクとコンプライアンス</p> <p>AWS Systems Manager のよくある質問</p> <p>https://aws.amazon.com/jp/systems-manager/faq/</p>																			

【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

【AWS FISCC安全対策基準対応リファレンス】からの引用					参考情報	【AWS FISCC安全対策基準対応リファレンス】からの引用					参考情報	【AWS FISCC安全対策基準対応リファレンス】からの引用					参考情報
実施単位	規格	形式の名称	AWS	対応	対応の状況	対応の状況	対応の状況	対応の状況	対応の状況	対応の状況	対応の状況	対応の状況	対応の状況	対応の状況	対応の状況	対応の状況	
実48	10	-	○	-	-	-	-	-	-	-	-	-	-	-	-	-	
					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、直営に管理されています。権限を付与されたスタッフは2 要員認証を最長2 回続いて、データセンターのフロアにアクセスします。サーバールーム直営地の物理アクセスシステムは、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、閉鎖路テレビ(CCTV) カメラで監視されています。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 への要請のため、監査中に外部の独立監査人によって確認されます。						設定を変更し、変更を記録維持するには、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変更を行うと、変更を繰り返す可能性があります。静的構成管理では、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アプリケーション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 サービスの構成を変更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更する。または変更を行うと手動で変更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この詳細レベルを変更し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データを減らしたりすることができ、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機能の書き換えを行う場合、AWS AppConfig を使用して、環境全体での書き換えを行うことができます。AWS では、以下のような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)のパイプラインを構築できます。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。そのすることで、構成変更の記録、構成変化の他のリソースへの影響、AWS Config Rules およびAWS Config コンジョイントマスタックを使用しと監視れる。または登録された変更との監視管理を行います。AWS では、以下のような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)の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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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限定した時間にもスクリプトを実行する。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 を使用して、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上の優先順位の高いイベントが実行されている時期を通知します。アクティビティを監視して、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、変更に対して特報ログがオープンであるかどうかとしてあるか、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、カレンダーの予定に沿って実行されるように設定できます。AWS Systems Manager マニファストシステムは、AWS SDN 環境で Amazon 認定 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						

【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

「AWS FISCC安全対策基準対応リファレンス」からの引用				参考情報		「AWS FISCC安全対策基準対応リファレンス」からの引用				参考情報	
項目番号	注釈	形式の注釈	形式の注釈	AWSの対応状況		追加情報が提供すべき内容					
第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。機械的メンテナンス手間は資格を持っている担当者が実行し、必要に応じてメンテナンスジョブに当てて完了されます。 また、問題の速やかな特定を可能にするため、電氣的、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。これは継続的な監視ツールと、建物管理および電氣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、設備の運用に関する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・物理アクセス設計 https://aws.amazon.com/jp/compliance/data-center/control/	
第55	-	○	-	AWS はサービスの利用状況を継続的にモニタリングし、オペラビリティ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、少なくとも月次及びキャパシティ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、機械的故障、停電、地震などのリスクを軽減するために活用されています。 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 Webサイト: AWSのコントロール・セキュリティ設計 https://aws.amazon.com/jp/compliance/data-center/control/	
第56	-	○	-	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事前認証を最低2回行って、データセンターのフロアにアクセスします。サーバー設置場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、閉鎖テレビ(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、法的または契約関係により30日間に制限される場合もあります。AWSは、このような特徴を必要とする正規の顧客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。	-	-				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/control/#Physical_Access	
第57	-	○	-	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事前認証を最低2回行って、データセンターのフロアにアクセスします。サーバー設置場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、閉鎖テレビ(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、法的または契約関係により30日間に制限される場合もあります。AWSは、このような特徴を必要とする正規の顧客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。	-	-				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/control/#Physical_Access	
第58	-	○	-	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、権限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ます。アクセスの申請が設定されます。申請は権限を持つ人物のみが審査して承認し、請求した期間が過ぎた後は、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事前認証を最低2回行って、データセンターのフロアにアクセスします。サーバー設置場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、閉鎖テレビ(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、法的または契約関係により30日間に制限される場合もあります。AWSは、このような特徴を必要とする正規の顧客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。	-	-				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/control/#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

「AWS FISCC安全対策基準対応リファレンス」からの引用				「AWS FISCC安全対策基準対応リファレンス」からの引用		「AWS FISCC安全対策基準対応リファレンス」からの引用	
基本構成	役割	対応の主体		参考情報	お客様が確認すべき内容	参考情報	確認情報
AWSの構成状況							
第59	-	○	-		-		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/
セキュリティを確保すべき領域での商業に関する管理は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欄に入場を許可され、権限を有するスタッフの関に付き添い待ちます。AWS は、そのような権限に対して正副のセキュリティエンジニアがある従業員や機器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。従業員がこれらの情報を必要とする機会を発生すると、その場に 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、そのアクセスは速やかに取り消されます。 AWS データセンターへの物理的アクセスは、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、該情報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、対応優先順位の決定、および決定された処理を実施していく責任を担っています。データセンターのアクセスを監視、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、対応優先順位の決定、コンサルティング、分析、迅速を行い、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。							
第60	-	○	-		-		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/
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。 現場管理 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。これは継続的な監視ツールと、建物管理および電気的設備の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、設備の運用に関するの継続性が保たれています。 CCTV サーバーール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、記録およびビデオファイルにアクセス可能な場所に格納されます。 データセンターのコントロールポイント 物理的アクセスは、建物の入り口において、サーベイルランスシステム、侵入検知システム、その他の電子のシステムを用いて、専門の保安要員によって厳密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。サーバーールへの入り口は、ドアが閉じ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おけ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。サーバーール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措置で保護されています。これらのデバイスは、許可されたドアが閉じ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							
第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。	-	-
第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。	-	-
第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。	-	-
第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。	-	-
第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。	-	-
第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。	-	-
第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。	-	-
第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。	-	-
第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。	-	-
第70	-	○	○		お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報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、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たいことができます。 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_39/compliance/NIST_Cybersecurity_Framework_CSF.pdf
第71	-	○	○		お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報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、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たいことができます。 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/ ）	【推奨】金融機関にて、BCP/DRに関連して以下の対策を検討する必要があります。 【対策例】 ■AWSでBCP/DRで取り巻く複雑な環境と災害対策の方法設計 ・AWSではBCP/DRの構築として、マルチリージョンやマルチAZ等のファシリティと、それらを金融機関側のアプリケーションと適切に組み合わせ、RTOなどの要求水準を考慮して設計ください。 ■バックアップシステムの少人数での運用とデュアル権限 ■インシデントの一次受け付けや通報時の責任分担の明確 ・インシデントの重要度に基づいて、エスカレーションルール策定(重要度は会話が1報告)など ■定期的に切磋琢磨の実施や、バックアップデータからサーバーを構築するなどの復旧訓練 【参考文献、参照URL】 ・AWSのBCPやDRの考え方は以下のURLを参照 「ビジネスの継続性と災害復旧」 https://aws.amazon.com/jp/compliance/data-center/controls/ ・AWSのリージョンやアベイラビリティゾーンについては以下のURLを参照 「グローバルインフラストラクチャリージョンとAZ」 https://aws.amazon.com/jp/about-aws/global-infrastructure/regions_az/?p=ng&loc=2	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_39/compliance/NIST_Cybersecurity_Framework_CSF.pdf
AWS における電気的インフラストラクチャ、機械的な高い自動化、物理的な高いプロセス、優れた人員を雇用すると、お客様の側で処理や発生した場合でも、それを最小限に抑え、該当イベントから迅速に回復できます。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開を目的として開発された、以下の3フェーズのプロトコルが詳しく記載されています。 ・アクティブレスポンスと通知のフェーズ ・通知のフェーズ ・再構成のフェーズ このプロトコルによって、AWS がシステムの問題と再開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、取り返しの利かない事態を最小限に抑え、エラーや事故に起因するシステムの稼働停止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機能を維持しています。各データセンターは、物理、電気、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。コンポーネントは冗長に設計して、少なくとも1つのバックアップコンポーネント(n+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ない他のすべてのコンポーネントが障害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になてトラフィックを受信しています。「フォールト」状態のデータセンターは利用できません。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。							

【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

【AWS FISCC緊急対応関係基幹対応リファレンス】からの引用					【AWS FISCC緊急対応関係基幹対応リファレンス】からの引用					【AWS FISCC緊急対応関係基幹対応リファレンス】からの引用				
緊急度	状態	対応の主体		AWSの対応状況	参考情報	対応の主体		AWSの対応状況	参考情報	対応の主体		AWSの対応状況	参考情報	対応の主体
		AWS	お客様											
表71	4	-	○	-	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たインシデント管理アプローチを使用しています。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行われます。さらに、Amazon のセキュリティディチームおよびサービスチームは、お客様への確信的な影響の無視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関与する責任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共同作成します。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				(表71 記載行を参照)	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-workload-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				
					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、重要な通知をより簡単に把握できます。 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。設定されたヘルムスチェックによって、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、事業継続のチェックとルーティンワークロード機能を使用して、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回復を組織にも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/re_planning_for_recovery_auto_recovery.html				(表71 記載行を参照)	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 FISCC 信頼性の柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/fsl/main/doc/fsi-lens-for-fisc/reliability.md				
表71	5	-	○	-	回復すべきパターンは、まれにしか実行されない復旧経路を作成することで。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て、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簡単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情報が不十分になり、セカンダリデータストアの障害は、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。エラー一連がうまくいくのは簡単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/リターンを確認して定期的にテストできます。復旧経路が可能な場合や発生するかもしれない復旧経路が正常に機能するという確信を持つには、本組織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、その必要性に照らして、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/re_planning_for_recovery_dr_tested.html			(表71 記載行を参照)	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 FISCC 信頼性の柱 https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute/fsl/main/doc/fsi-lens-for-fisc/reliability.md				
表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たインシデント管理アプローチを使用しています。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行われます。さらに、Amazon のセキュリティディチームおよびサービスチームは、お客様への確信的な影響の無視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関与する責任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共同作成します。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上で実行するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様に実施します。 AWS サポートは、経営層または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ます。質問可能な時間帯およびバーチャライズされたサポートを受け取ることができます。 AWS サポートの詳細については以下URLをご参照ください。（ https://aws.amazon.com/jp/premiumsupport/）			(表72 記載行を参照)	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 の実装 https://d1.compliance.nist.gov/whitepaper/ja_jp/complianceNIST_Cybersecurity_Framework_CSF.pdf				
					AWS のサポートは、経営層または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ます。質問可能な時間帯およびバーチャライズされたサポートを受け取ることができます。 AWS サポートの詳細については以下URLをご参照ください。（ https://aws.amazon.com/jp/premiumsupport/）				(表72 記載行を参照)	■障害状況の確認・記録 ■AWS以下のサービスを使用し、AWSサービスの障害状況を確認します。一定期間記録されるため、必要に応じて復旧を保持します ■AWSサービス障害状況: AWS Health ・各サービスの障害状況: CloudWatchストロクス(障害確認、記録、ログ管理) ・システムのコログ: CloudWatchログ(事前に出力設定が必要) ・API操作ログ: CloudTrail(CloudWatchログに出力を連携) ■検出・通知 システムに問題がある動きがある場合に、速やかに検出・通知するために、以下機能を設定します ・AWS Healthの検出・通知: AWS User Notifications ・CloudWatchストロクス・ログの検出・通知: CloudWatchアラーム				
表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、重要な通知をより簡単に把握できます。 https://docs.aws.amazon.com/ja_jp/health/latest/ug/what-is-aws-health.html			(表72 記載行を参照)	AWS Health ユーザーガイド https://docs.aws.amazon.com/ja_jp/health/latest/ug/what-is-aws-health.html					
表72	9	-	○	-	AWS Health Dashboardのサービス一覧では、過去12カ月のAWSサービスの利用率が表示されます。 https://health.aws.amazon.com/health/status			(表72 記載行を参照)	AWS Health Dashboard - サービスの状況 https://health.aws.amazon.com/health/status ・左記のとおり、AWS Health Dashboardを活用することで、状況把握が可能です。 ・AWSサービス利用率の傾向や継続時間の実績を踏まえ、必要十分なシステム構成であることを確認します。					
表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、イベントが起る前、イベントの際中、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、最近の進展、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、感染症の世界的な流行の発生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業務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ージョンに移動するために、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機関に提言しています。 【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。 https://aws.amazon.com/jp/compliance/soc-faq/	【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、イベントが起る前、イベントの際中、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、最近の進展、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、感染症の世界的な流行の発生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業務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ージョンに移動するために、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機関に提言しています。 【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。 https://aws.amazon.com/jp/compliance/soc-faq/	お客様がAWS上で実行するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様に実施します。 AWS サポートは、経営層または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ます。質問可能な時間帯およびバーチャライズされたサポートを受け取ることができます。 AWS サポートの詳細については以下URLをご参照ください。（ https://aws.amazon.com/jp/premiumsupport/）			(表73 記載行を参照)	AWS Well-Architected フレームワーク FSI Lens for FISCC 信頼性の柱 ■AWS以下のサービスを使用し、AWSサービスの障害状況を確認します。一定期間記録されるため、必要に応じて復旧を保持します ■AWSサービス障害状況: AWS Health ・各サービスの障害状況: CloudWatchストロクス(障害確認、記録、ログ管理) ・システムのコログ: CloudWatchログ(事前に出力設定が必要) ・API操作ログ: CloudTrail(CloudWatchログに出力を連携) ■検出・通知 システムに問題がある動きがある場合に、速やかに検出・通知するために、以下機能を設定します ・AWS Healthの検出・通知: AWS User Notifications ・CloudWatchストロクス・ログの検出・通知: CloudWatchアラーム			

【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

「AWS FISCC安全対策実施事例対応リファレンス」からの引用					「AWS FISCC安全対策実施事例対応リファレンス」からの引用					「AWS FISCC安全対策実施事例対応リファレンス」からの引用				
記事番号	図表	形式の主な			参考情報		お客様が対策すべき内容		参考情報		AWS			
図76	3	-	○	-			AWS では、社内レポート機能を使用せずに、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、特定のコンプライアンスに準拠し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、アカウントが複雑な環境となります。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。		【概要】AWS 上での本番環境とテスト環境の分離方法・機能としては、AWS アカウントレベルでの分離と、VPC によるネットワークワークレベルでの分離が大きく挙げられます。VPC によるネットワークワークレベルでの分離は一般に権限管理が複雑になる構図にあるため、アカウントレベルでの分離が強く推奨されます。		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/aws-account-management-and-separation.html		【対策例】(1) クラウドサービスで構築するシステムについて、完全に本番環境とテスト環境を分離する方法や機能 本番環境・テスト環境はAWSアカウントレベルで分離し、それぞれのアカウント内に必要なリソースを作成します。		「AWS FISCC安全対策実施事例対応リファレンス」からの引用			
									(2) 本番環境とテスト環境を分離した際のプログラムやデータ等の連携方法 AWSアカウント間のデータ連携方法として、S3/ワット活用する方法等が考えられます。					
									また、Amazon マシンイメージのように、他のアカウントに共有する機能を備えているサービスもあります。(※1)					
									【参考文献、参照URL】(※1) Amazon Elastic Compute Cloud ・特定の AWS アカウントとの AMI の共有 https://docs.aws.amazon.com/ja_jp/AWSSEC2/latest/UserGuide/sharingamis-explicit.html					
図77	-	-	○	-			お客様がAWS上で実行するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の情報を用いて、お客様にて実施します。							
図78	-	-	○	-			お客様がAWS上で実行するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の情報を用いて、お客様にて実施します。							
図79	-	-	○	-			お客様がAWS上で実行するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の情報を用いて、お客様にて実施します。							
図80	-	-	○	-			お客様がAWS上で実行するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の情報を用いて、お客様にて実施します。							
図81	-	-	○	-			お客様がAWS上で実行するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の情報を用いて、お客様にて実施します。							
図82	-	-	○	-	(図82 記載行を参照)		お客様がAWS上で実行するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の情報を用いて、お客様にて実施します。		【概要】クラウド利用の場合には、廃棄計画について確認する必要があります。 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。					
									【参考文献、参照URL】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/detstoringadatapractice/					
図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。		(図82 記載行を参照)		クラウドにおける安全なデータの廃棄			
							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/detstoringadatapractice/				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/detstoringadatapractice/			
図83	-	-	○	-			【概要】AWSが利用しているデータセンターは、システム廃棄時の情報漏えい防止対策について対応しています。		【概要】システム廃棄時の情報漏えい防止対策を講ずる必要があります。 AWSでは、デバイスの設置、修理、および廃棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。金融機関が適切な手段によってデータをさらに保護することが推奨されています。					
							【対策例】AWS データセンターにおけるメディアの廃棄は、セキュリティを念頭に置いて設計されており、厳格により具体的セキュリティが実施されています。ユーザーデータの廃棄に使用されるメディアストレージデバイスはAWSによって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWSでは、デバイスの設置、修理、および廃棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製造時に渡した場合は、NST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に廃止するまでAWSの規制が強制されることはありません。AWSで扱われるメディアはワブ処理もしくは再組処理され、AWSのセキュアゾーンを離れる前に物理的に破壊されます。AWSの第三者レポートに文書化されているように、AWS データセンターに対する第三者の検証によって、AWS がセキュリティ認証を取得し必要となるルールを確立するためのセキュリティ対策を適切に実施していることが保証されます。お客様はこうした第三者のレポートをAWS Artifactから入手することが可能です。			【参考文献、参照URL】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/				
図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、優れた人員を採用すると、お客様の前で故障や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記載されています。		お客様がAWS上で実行するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の情報を用いて、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			
							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。		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も最も可用性を実現するために重要な要素となります。		https://d1.awsstatic.com/whitepapers/ja_jp/compliance/NIST_Cybersecurity_Framework_CSF.pdf			
							•アデ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、エラーや作業遅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隔離に機能している場合もアクティブになります。第一階層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を必要とトランザクションを提供しています。「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、残りのサードパーティのバックアップの可用性が数分で十分な回復能力が確保されています。							
図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、優れた人員を採用すると、お客様の前で故障や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記載されています。		お客様がAWS上で実行するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の情報を用いて、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			
							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。		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も最も可用性を実現するために重要な要素となります。		https://d1.awsstatic.com/whitepapers/ja_jp/compliance/NIST_Cybersecurity_Framework_CSF.pdf			
							•アデ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、エラーや作業遅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隔離に機能している場合もアクティブになります。第一階層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を必要とトランザクションを提供しています。「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、残りのサードパーティのバックアップの可用性が数分で十分な回復能力が確保されています。							

【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

「AWS FISCC安全対策実施対応リファレンス」からの引用				「AWS FISCC安全対策実施対応リファレンス」からの引用				「AWS FISCC安全対策実施対応リファレンス」からの引用			
実施単位	役割	対応の主体		AWSの対応状況	参考情報	お客様が実施すべき内容	参考情報	対応の主体		AWSの対応状況	参考情報
実86	-	○	○					実87	-		
<p>AWS における高可用性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、優れた人員を有する。 お客様の需要と信頼性要件を満たす際でも、それを最小限に引き、該当イベントから迅速に回復できます。 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。</p> <p>・アクティベーションと通知のフェーズ</p> <p>・復旧のフェーズ</p> <p>・再構成のフェーズ</p> <p>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、取り組みの有用性が最大限に高まり、エラーや不審な点に起因するシステムの信頼性が時間単位で最小限に抑えられます。 AWS は、すべてのリソースとわたる完全なセキュリティ機能の範囲を継続管理しています。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(n+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故障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つ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、残りのサイトとトラフィックの急激な増えを必要としない復旧能力が確保されています。</p>											
実87	-	○	○	各データセンター間では物理的に離れており、冗長性のある電源とネットワークを備えています。 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クを接続する。完全な冗長性を持つ専用メトロファイバー上に構築された、高帯幅、低レイテンシーのネットワークに相互接続されています。		お客様がAWS 上で実施するシステムおよびサービスの管理は、AWS が提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	【概要】オンプレミスと同様、特定システムで重要な装置には、故障発生時の迅速な対応のため、オンプレミス環境に回線の予備の用意が望ましいとされています。				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
<p>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。</p> <p>AWS は、堅牢な継続性計画を実施する機能をお客様に提供しています。たとえば、調整なサーバーインスタンスバックアップの利用、データの冗長レプリケーション、マルチリージョン/アベイラビリティゾーンでのデプロイアーキテクチャなどです。</p>											
実88	-	○	○	(実87と同様)		お客様がAWS 上で実施するシステムおよびサービスの管理は、AWS が提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	【概要】オンプレミスと同様、特定システムでの重要な装置には、故障発生時の迅速な対応のため、オンプレミス環境に回線の予備の用意が望ましいとされています。				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ゾーン
実89	-	-	○	-		お客様がAWS 上で実施するシステムおよびサービスの管理は、AWS が提供する機能および情報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 上で実施するシステムおよびサービスの管理は、AWS が提供する機能および情報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 上で実施するシステムおよびサービスの管理は、AWS が提供する機能および情報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 上で実施するシステムおよびサービスの管理は、AWS が提供する機能および情報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 上で実施するシステムおよびサービスの管理は、AWS が提供する機能および情報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 上で実施するシステムおよびサービスの管理は、AWS が提供する機能および情報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 上で実施するシステムおよびサービスの管理は、AWS が提供する機能および情報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 上で実施するシステムおよびサービスの管理は、AWS が提供する機能および情報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 上で実施するシステムおよびサービスの管理は、AWS が提供する機能および情報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 上で実施するシステムおよびサービスの管理は、AWS が提供する機能および情報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99	-	○	○	AWS における高可用性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、優れた人員を有する。 お客様の需要と信頼性要件を満たす際でも、それを最小限に引き、該当イベントから迅速に回復できます。 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。 <p>・アクティベーションと通知のフェーズ</p> <p>・復旧のフェーズ</p> <p>・再構成のフェーズ</p> <p>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、取り組みの有用性が最大限に高まり、エラーや不審な点に起因するシステムの信頼性が時間単位で最小限に抑えられます。</p> <p>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、事前の計画、テスト、承認され、充分な情報が提供されます。変更の実行前段階への入力は厳格、最も影響の大きいリソースの即時情報提供が開始されます。デプロイは「即ち」のシステムでテストされ、影響が評価できるよう継続的にモニタリングされます。</p> <p>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。</p> <p>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。</p> <p>2.影響を最小限にするために、変更をよりローバルバックアップ手続の実施を計画します。</p> <p>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。</p> <p>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</p>	お客様がAWS 上で実施するシステムおよびサービスの管理は、AWS が提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	【概要】オンプレミスと同様、特定システムでの重要な装置には、故障発生時の迅速な対応のため、オンプレミス環境に回線の予備の用意が望ましいとされています。				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 への関係 https://d1.awsstatic.com/whitepapers/ja_JP/compliance/NIST_Cybersecurity_Framework_CSF.pdf AWS CloudFormationでは、アプリケーションを動かす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便化できます。 AWS Step Functionsでは、順番、再試行、並列化、サービス統合、可観測性などを管理し、ワークフローが順番どおりに実行されていることを確認できます。また、ビルトインの try/catch、再試行、ロールバック機能を用いることで、定義されたビジネスロジックに基づいてエラーや例外に自動的に対応できます。 Amazon EventBridgeでは、イベントの取り込み、フィルタリング、変換、および駆動をカスタムコードを記述することなく、行うことができます。スキーマ検出機能を使用し、イベントバスから抽出されたスキーマをレジストリに自動的に追加できます。	

【AWS FISCC安全対策実施事例対応リファレンス】からの引用					「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
実施事例	図数	対応の主体			AWSの対応状況	参考情報
		お客様	パートナー	ベンダー		
実99	3	-	○	-	AWSの対応状況	お客様が実施すべき内容
					参考情報	成立情報

實務基準

© 2023, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

「AWS FISC安全対策標準対応リファレンス」からの引用					付加情報
基準番号	技術	対応の主体		AWSの対応状況	
		AWS	お客様		
監1	1	-	○	<p>・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。</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>【概要】</p> <p>責任共有モデルに基づき金融機関等の責任範囲となる部分はシステム上の設定等(AWSのクラウドサービスを含む)を参照して監査を実施する必要がある。一方、AWSの責任範囲に対する監査は、データセンターへの立ち入りを認めていない等の制約があることから、第三者保証による報告書または第三者認証に関する情報の確認により実施する等の代替手段をとる必要がある。これらの制約を踏まえ、特に、個人情報を取り扱う情報システムの利用及び個人情報へのアクセスの監視状況は責任共有モデルを考慮したシステム監査を行う必要がある。</p> <p>【参考文献、参照URL】</p> <ul style="list-style-type: none">・責任共有モデル https://aws.amazon.com/jp/compliance/shared-responsibility-model/・AWSコンプライアンスプログラム https://aws.amazon.com/jp/compliance/programs/
	2	-	○	-	-
	3	-	○	<p>・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。</p> <p>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。</p>	<p>【概要】</p> <p>AWS上に存在する情報の取扱い金融機関等の責任範囲であり、金融機関側でのコントロールが求められる。特に機微(センシティブ)情報を扱う場合は、より客観性が求められることから、外部の専門機関を活用し評価することも視野に入れる。</p> <p>【参考文献、参照URL】</p> <ul style="list-style-type: none">・責任共有モデル https://aws.amazon.com/jp/compliance/shared-responsibility-model/
	4	-	○	<p>・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。</p> <p>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。</p> <p>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。</p>	<p>【概要】</p> <p>AWSの公開文書として金融機関等や監査人がAWSに尋ねる可能性が高い質問への回答が用意されており、システム監査の指摘事項について検証する際には、これらも確認することが望ましい。</p> <p>【参考文献、参照URL】</p> <ul style="list-style-type: none">・『コンプライアンスに関するよくある質問』 1.AWSの年次ベンダー/サプライヤー/デューデリジェンスアンケートに回答するための最良の方法は何ですか？ https://aws.amazon.com/jp/compliance/faq/
	5	-	○	<p>・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。</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>【概要】</p> <ul style="list-style-type: none">・AWSの内部統制の評価は、主に第三者保証による報告書または第三者認証に関する情報の確認により実施する。・SOC1は財務報告に係る内部統制の評価を目的としており、会計監査や内部統制監査において有用と言える。一方、SOC2は財務報告以外に係る内部統制の評価を目的としており、より一般的なセキュリティ監査や安全性・信頼性の確認等において有用と言える。・SOCレポートをはじめとした第三者保証による報告書はAWS Artifactを通じて、AWSとNDAを締結したうえで閲覧することができる。・AWSはデータセンター施設の管理を目的として、事業者への再委託を実施しており、その管理プロセスは、SOCおよびISO27001へのAWSの継続的な準拠の一環として、独立した監査人によって確認されている。 <p>※SOCレポートの利用に際しては、統26-3も参照</p> <p>【参考文献、参照URL】</p> <ul style="list-style-type: none">・SOC コンプライアンス - アマゾン ウェブ サービス (AWS) https://aws.amazon.com/jp/compliance/soc-faqs/・AWS Artifact https://aws.amazon.com/jp/artifact/・補助処理者と提携事業者