「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」（2020年9月公開）対応

2022年 2月

作成： 株式会社エヌ・ティ・ティ・データ
SCSK株式会社
TIS株式会社
シンプレクス株式会社
株式会社電通国際情報サービス
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2020年9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。

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
-	-	-	-	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 (更新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/jp/compliance/shared-responsibility-model/	-
統1		-	○	-	-
統2		-	○	-	-
統3		-	○	-	-
統4		-	○	-	-
統5		-	○	-	-
統6		-	○	-	-
統7		-	○	-	-
統8		-	○	-	-
統9		-	○	-	-
統10		-	○	-	-
統11		-	○	-	-
統12		-	○	-	-
統13		-	○	-	-
統14		-	○	-	-
統15		-	○	-	-
統16		-	○	-	-
統17		-	○	-	-
統18		-	○	-	-
統19		-	○	-	-
統20	1	-	○	-	-
統20	2	-	○	-	-

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
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適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-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/ 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学歴、雇用歴、場合によっては経歴の確認を、採用手続きの一環として実施しています。新たに採用した従業員には体系的な入社時研修を行い、Amazon のツール、プロセス、システム、ポリシー、手順について熟知させるようにします。 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、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。 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厳重な監視 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/	[概要] 「AWSとは」の全般的な説明については、「AWS によるクラウドコンピューティング(注1)」を参照する。AWSを利用した導入事例に関しては、「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「カスタマー支援(注4　英語)」を参照する。 AWSの客観的な評価に関する第三者認証(SOCレポート入手など)に関しては、「AWS Artifact(注5)」「AWS Artifactのよくある質問(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://d1.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/

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		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永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報告書 AWS System and Organization Controls（SOC）報告書は、 AWS が重要なコンプライアンス管理および目標をどのように達成しているかを示す、独立した第三者による調査報告書です。 これらの報告書の目的は、運用およびコンプライアンスをサ ポートするために確立された AWS の統制を、お客様、および、お客様の監査人にご理解いただくことです。AWS の SOC 報告書には次の 3 種類があります。 • SOC 1: 財務報告に係る内部統制（ICFR）に関連する可 能性がある AWS の統制環境に関する情報のほかに、ICFR の有効性の評価に関する情報を提供します。 • SOC 2: お客様および業務上の必要性があるサービスユーザーに、システムセキュリティ、可用性、および機密性に 関連するAWSの統制環境についての独立した評価を提供します。 • SOC 3: お客様および業務上の必要性があるサービスユーザーに、 AWSの統制環境についての独立した評価を提供し、AWS の内部情報を開示せずにシステムセキュリティ、 可用性、および機密性に関連する情報を提供します。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-(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-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/	-

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		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永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報告書 AWS System and Organization Controls（SOC）報告書は、 AWS が重要なコンプライアンス管理および目標をどのように達成しているかを示す、独立した第三者による調査報告書です。 これらの報告書の目的は、運用およびコンプライアンスをサ ポートするために確立された AWS の統制を、お客様、および、お客様の監査人にご理解いただくことです。AWS の SOC 報告書には次の 3 種類があります。 • SOC 1: 財務報告に係る内部統制（ICFR）に関連する可 能性がある AWS の統制環境に関する情報のほかに、ICFR の有効性の評価に関する情報を提供します。 • SOC 2: お客様および業務上の必要性があるサービスユーザーに、システムセキュリティ、可用性、および機密性に 関連するAWSの統制環境についての独立した評価を提供します。 • SOC 3: お客様および業務上の必要性があるサービスユーザーに、 AWSの統制環境についての独立した評価を提供し、AWS の内部情報を開示せずにシステムセキュリティ、 可用性、および機密性に関連する情報を提供します。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)	-	○	-	[概要] AWSで提供されているサービスの可用性については、「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。 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4)」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://aws.amazon.com/jp/compliance/shared-responsibility-model/

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		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学歴、雇用歴、場合によっては経歴の確認を、採用手続きの一環として実施しています。新たに採用した従業員には体系的な入社時研修を行い、Amazon のツール、プロセス、システム、ポリシー、手順について熟知させるようにします。 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、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。 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永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報告書 AWS System and Organization Controls（SOC）報告書は、 AWS が重要なコンプライアンス管理および目標をどのように達成しているかを示す、独立した第三者による調査報告書です。 これらの報告書の目的は、運用およびコンプライアンスをサ ポートするために確立された AWS の統制を、お客様、および、お客様の監査人にご理解いただくことです。AWS の SOC 報告書には次の 3 種類があります。 • SOC 1: 財務報告に係る内部統制（ICFR）に関連する可 能性がある AWS の統制環境に関する情報のほかに、ICFR の有効性の評価に関する情報を提供します。 • SOC 2: お客様および業務上の必要性があるサービスユーザーに、システムセキュリティ、可用性、および機密性に 関連するAWSの統制環境についての独立した評価を提供します。 • SOC 3: お客様および業務上の必要性があるサービスユーザーに、 AWSの統制環境についての独立した評価を提供し、AWS の内部情報を開示せずにシステムセキュリティ、 可用性、および機密性に関連する情報を提供します。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/	-

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
統20	3-(5)	-	○	・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	[概要] 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 カスタマーアグリーメント(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。 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へのリンクがまとまっている。S3サービスにおける暗号化については、「暗号化を使用したデータの保護(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)」に各サービス上へのリンクがまとまっている。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。 [参考文献、参照URL] ○注 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.html 5　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-(6)	-	○	・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。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。	[概要] 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 カスタマーアグリーメント(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。 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へのリンクがまとまっている。S3サービスにおける暗号化については、「暗号化を使用したデータの保護(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)」に各サービス上へのリンクがまとまっている。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。 [参考文献、参照URL] ○注 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.html 5　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/

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
統20	3-(7)	-	○	SOC報告書 AWS System and Organization Controls（SOC）報告書は、 AWS が重要なコンプライアンス管理および目標をどのように達成しているかを示す、独立した第三者による調査報告書です。 これらの報告書の目的は、運用およびコンプライアンスをサ ポートするために確立された AWS の統制を、お客様、および、お客様の監査人にご理解いただくことです。AWS の SOC 報告書には次の 3 種類があります。 • SOC 1: 財務報告に係る内部統制（ICFR）に関連する可 能性がある AWS の統制環境に関する情報のほかに、ICFR の有効性の評価に関する情報を提供します。 • SOC 2: お客様および業務上の必要性があるサービスユーザーに、システムセキュリティ、可用性、および機密性に 関連するAWSの統制環境についての独立した評価を提供します。 • SOC 3: お客様および業務上の必要性があるサービスユーザーに、 AWSの統制環境についての独立した評価を提供し、AWS の内部情報を開示せずにシステムセキュリティ、 可用性、および機密性に関連する情報を提供します。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] 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。 [参考文献、参照URL] ○注 1 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Answers_to_Key_Compliance_Questions_JP.pdf 2　https://aws.amazon.com/jp/compliance/data-center/controls/ 3　https://aws.amazon.com/jp/compliance/soc-faqs
統20	3-(8)	-	○	・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。 - 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。 - 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。 - 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。 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。 - 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。 - 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。 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/	[概要] 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。 [例] AWSでは、移行方式の例として以下の6つを挙げている。(6R) ・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 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。 [参考文献、参照URL] ・【【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
統20	3-(9)	-	○	・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。 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/ 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/	[概要] 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。 [参考文献、参照URL] ○注 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/

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
統20	3-(10)	-	○	・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	[概要] 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)。 (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。 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。 [参考文献、参照URL] ○注 1　https://aws.amazon.com/jp/agreement/ 2　注１のリンクより日本語版アクセス可能 3　https://aws.amazon.com/jp/legal/service-level-agreements/
統20	3-(11)	-	○	・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/ 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ています。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置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/ 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。 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、および破棄 (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。 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] AWSの契約終了に関しては、「AWS アカウントを解約するにはどうすればよいですか?(注1)」を参照する。 [参考文献、参照URL] ○注 1　https://aws.amazon.com/jp/premiumsupport/knowledge-center/close-aws-account/ -
統20	3-(12)	-	○	・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/	[概要] 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。 AWS側の関連する対応に関して、データプライバシー全般については、「データプライバ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。 [参考文献、参照URL] ○注 1　https://aws.amazon.com/jp/compliance/data-privacy-faq/ 2　https://aws.amazon.com/jp/compliance/iso-27018-faqs/

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
統20	3-(13)	-	○	・AWS では 160 種類を超えるクラウドサービスについて従量制料金を適用しています。 AWS では必要な個々のサービスにのみ、サービスを使用する期間だけお支払いいただき、長期契約や複雑なライセンスは必要ありません。 サービスを消費した分だけ支払い、サービスの使用を停止したときの追加コストや解約料金はありません。 https://aws.amazon.com/jp/pricing/	[概要] サービス料金については、「AWS 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、「30 の目的別 クラウド構成と料金試算例(注3)」を参照する。 [例] 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「EC2」(注４)、ストレージ「S3」(注５)、データベース「RDS」(注６)の料金に関する記述は、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。 [参考文献、参照URL] ○注 1　https://aws.amazon.com/jp/pricing/ 2　https://calculator.aws/#/ 3　https://aws.amazon.com/jp/cdp/ 4　https://aws.amazon.com/jp/ec2/pricing/ 5　https://aws.amazon.com/jp/s3/pricing/ 6　https://aws.amazon.com/jp/rds/pricing/
統20	3-(14)	-	○	・2017年11月より日本のお客様に向けて「日本準拠法に関する AWS カスタマーアグリーメント変更契約」の手続きが可能な新機能の提供を開始しました。これにより、AWS Artifact を通じて日本準拠法に関する AWS カスタマーアグリーメント変更契約をリアルタイムに締結または終了することが可能となっています。日本準拠法に関する AWS カスタマーアグリーメント変更契約とは、現在お客様がご利用中の AWS アカウントに適用されている、 AWS カスタマーアグリーメントの準拠法および管轄裁判所を変更する契約を指します。この契約を有効にすることで、 AWS カスタマーアグリーメントの準拠法を日本法に変更し、更に、同契約に関するあらゆる紛争に関する第一審裁判所を東京地方裁判所に変更することができます。 従来、AWSカスタマーアグリーメントの準拠法および管轄裁判所を変更する際に、その都度、書面で契約を締結して頂く必要がありましたが、AWSアカウントのマネジメントコンソールからお客様ご自身で受諾（有効に）することで、お客様の手間を省略することが可能となっています。 https://aws.amazon.com/jp/blogs/news/how-to-change-aws-ca-by-artifact/	[概要] 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。 [参考文献、参照URL] ○注 1　https://aws.amazon.com/jp/agreement/ 2　https://console.aws.amazon.com/artifact
統20	4	-	○	-	-
統20	5	-	○	-	-
統20	6	-	○	-	-
統21	1, 2	-	○	・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 2017年11月より、日本のお客様に向けて「日本準拠法に関する AWS カスタマーアグリーメント変更契約」の手続きが可能な新機能の提供を開始しました。これにより、AWS Artifact を通じて日本準拠法に関する AWS カスタマーアグリーメント変更契約をリアルタイムに締結または終了することが可能となっています。日本準拠法に関する AWS カスタマーアグリーメント変更契約とは、現在お客様がご利用中の AWS アカウントに適用されている、 AWS カスタマーアグリーメントの準拠法および管轄裁判所を変更する契約を指します。この契約を有効にすることで、 AWS カスタマーアグリーメントの準拠法を日本法に変更し、更に、同契約に関するあらゆる紛争に関する第一審裁判所を東京地方裁判所に変更することができます。 https://aws.amazon.com/jp/blogs/news/how-to-change-aws-ca-by-artifact/	-
統21	3	-	○	-	-

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
統22	1	-	○	・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。 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。 従業員へのセキュリティ教育、トレーニング 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。 社員が個々の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。	[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。 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。 [参考文献、参照URL] ○注 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/
				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永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/	

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
				SOC報告書 AWS System and Organization Controls（SOC）報告書は、 AWS が重要なコンプライアンス管理および目標をどのように達成しているかを示す、独立した第三者による調査報告書です。 これらの報告書の目的は、運用およびコンプライアンスをサ ポートするために確立された AWS の統制を、お客様、および、お客様の監査人にご理解いただくことです。AWS の SOC 報告書には次の 3 種類があります。 • SOC 1: 財務報告に係る内部統制（ICFR）に関連する可 能性がある AWS の統制環境に関する情報のほかに、ICFR の有効性の評価に関する情報を提供します。 • SOC 2: お客様および業務上の必要性があるサービスユー ザーに、システムセキュリティ、可用性、および機密性に 関連するAWSの統制環境についての独立した評価を提供します。 • SOC 3: お客様および業務上の必要性があるサービスユー ザーに、 AWSの統制環境についての独立した評価を提供し、AWS の内部情報を開示せずにシステムセキュリティ、 可用性、および機密性に関連する情報を提供します。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	2	-	○	・AWSではISO/IEC 27001およびPCI DSSに則り、AWS環境への論理的なアクセスのために必要な手順やポリシーを定めています。 AWS 人事管理システムのオンボーディングワークフロープロセスの一環として、一意のユーザー ID が作成されます。デバイスプロビジョニングプロセスは、デバイスの ID を確実に一意にするうえで役立ちます。両方のプロセスとも、ユーザーアカウントまたはデバイスを確立するためのマネージャーの承認が含まれます。最初の認証は、プロビジョニングプロセスの一部としてユーザーに対面で提供されるとともに、デバイスにも提供されます。内部ユーザーは SSH パブリックキーをアカウントに関連付けることができます。システムカウントの認証は、リクエスタの ID を確認した後で、アカウント作成プロセスの一部としてリクエスタに提供されます。	-
統22	3	-	○	SOC報告書 AWS System and Organization Controls（SOC）報告書は、 AWS が重要なコンプライアンス管理および目標をどのように達成しているかを示す、独立した第三者による調査報告書です。 これらの報告書の目的は、運用およびコンプライアンスをサ ポートするために確立された AWS の統制を、お客様、および、お客様の監査人にご理解いただくことです。AWS の SOC 報告書には次の 3 種類があります。 • SOC 1: 財務報告に係る内部統制（ICFR）に関連する可 能性がある AWS の統制環境に関する情報のほかに、ICFR の有効性の評価に関する情報を提供します。 • SOC 2: お客様および業務上の必要性があるサービスユー ザーに、システムセキュリティ、可用性、および機密性に 関連するAWSの統制環境についての独立した評価を提供します。 • SOC 3: お客様および業務上の必要性があるサービスユー ザーに、 AWSの統制環境についての独立した評価を提供し、AWS の内部情報を開示せずにシステムセキュリティ、 可用性、および機密性に関連する情報を提供します。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23	1, 2	-	○	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。	[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。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。 [参考文献、参照URL] ○注 1 https://aws.amazon.com/jp/compliance/soc-faqs 2 https://aws.amazon.com/jp/compliance/data-center/controls/ 3 https://aws.amazon.com/jp/legal/service-level-agreements/

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
				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。 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永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報告書 AWS System and Organization Controls（SOC）報告書は、 AWS が重要なコンプライアンス管理および目標をどのように達成しているかを示す、独立した第三者による調査報告書です。 これらの報告書の目的は、運用およびコンプライアンスをサ ポートするために確立された AWS の統制を、お客様、および、お客様の監査人にご理解いただくことです。AWS の SOC 報告書には次の 3 種類があります。 • SOC 1: 財務報告に係る内部統制（ICFR）に関連する可 能性がある AWS の統制環境に関する情報のほかに、ICFR の有効性の評価に関する情報を提供します。 • SOC 2: お客様および業務上の必要性があるサービスユーザーに、システムセキュリティ、可用性、および機密性に 関連するAWSの統制環境についての独立した評価を提供します。 • SOC 3: お客様および業務上の必要性があるサービスユーザーに、 AWSの統制環境についての独立した評価を提供し、AWS の内部情報を開示せずにシステムセキュリティ、 可用性、および機密性に関連する情報を提供します。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/	

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
統24	1	-	○	・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。 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。 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。 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 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 2017年11月より同サービスにおいて、日本のお客様に向けて「日本準拠法に関する AWS カスタマーアグリーメント変更契約」の手続きが可能な新機能の提供を開始しました。これにより、AWS Artifact を通じて日本準拠法に関する AWS カスタマーアグリーメント変更契約をリアルタイムに締結または終了することが可能となっています。日本準拠法に関する AWS カスタマーアグリーメント変更契約とは、現在お客様がご利用中の AWS アカウントに適用されている、 AWS カスタマーアグリーメントの準拠法および管轄裁判所を変更する契約を指します。この契約を有効にすることで、 AWS カスタマーアグリーメントの準拠法を日本法に変更し、更に、同契約に関するあらゆる紛争に関する第一審裁判所を東京地方裁判所に変更することができます。従来、AWS カスタマーアグリーメントの準拠法および管轄裁判所を変更する際に、その都度、書面で契約を締結して頂く必要がありましたが、AWSアカウントのマネジメントコンソールからお客様ご自身で受諾（有効に）することで、お客様の手間を省略することが可能となっています。 https://aws.amazon.com/jp/blogs/news/how-to-change-aws-ca-by-artifact/ 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。 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。 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/ 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。	[概要] 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。 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。 [参考文献、参照URL] ○注 1　https://aws.amazon.com/jp/artifact/ 　　https://aws.amazon.com/jp/artifact/getting-started/ 2　https://aws.amazon.com/jp/about-aws/global-infrastructure/

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
				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。 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永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報告書 AWS System and Organization Controls（SOC）報告書は、 AWS が重要なコンプライアンス管理および目標をどのように達成しているかを示す、独立した第三者による調査報告書です。 これらの報告書の目的は、運用およびコンプライアンスをサ ポートするために確立された AWS の統制を、お客様、および、お客様の監査人にご理解いただくことです。AWS の SOC 報告書には次の 3 種類があります。 • SOC 1: 財務報告に係る内部統制（ICFR）に関連する可 能性がある AWS の統制環境に関する情報のほかに、ICFR の有効性の評価に関する情報を提供します。 • SOC 2: お客様および業務上の必要性があるサービスユーザーに、システムセキュリティ、可用性、および機密性に 関連するAWSの統制環境についての独立した評価を提供します。 • SOC 3: お客様および業務上の必要性があるサービスユーザーに、 AWSの統制環境についての独立した評価を提供し、AWS の内部情報を開示せずにシステムセキュリティ、 可用性、および機密性に関連する情報を提供します。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/	

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
統24	2	-	○	・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。 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。 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 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 2017年11月より同サービスにおいて、日本のお客様に向けて「日本準拠法に関する AWS カスタマーアグリーメント変更契約」の手続きが可能な新機能の提供を開始しました。これにより、AWS Artifact を通じて日本準拠法に関する AWS カスタマーアグリーメント変更契約をリアルタイムに締結または終了することが可能となっています。日本準拠法に関する AWS カスタマーアグリーメント変更契約とは、現在お客様がご利用中の AWS アカウントに適用されている、 AWS カスタマーアグリーメントの準拠法および管轄裁判所を変更する契約を指します。この契約を有効にすることで、 AWS カスタマーアグリーメントの準拠法を日本法に変更し、更に、同契約に関するあらゆる紛争に関する第一審裁判所を東京地方裁判所に変更することができます。従来、AWS カスタマーアグリーメントの準拠法および管轄裁判所を変更する際に、その都度、書面で契約を締結して頂く必要がありましたが、AWSアカウントのマネジメントコンソールからお客様ご自身で受諾（有効に）することで、お客様の手間を省略することが可能となっています。 https://aws.amazon.com/jp/blogs/news/how-to-change-aws-ca-by-artifact/ 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。 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。 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/ 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。	[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。 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である。 [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

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
				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。 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永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報告書 AWS System and Organization Controls（SOC）報告書は、 AWS が重要なコンプライアンス管理および目標をどのように達成しているかを示す、独立した第三者による調査報告書です。 これらの報告書の目的は、運用およびコンプライアンスをサ ポートするために確立された AWS の統制を、お客様、および、お客様の監査人にご理解いただくことです。AWS の SOC 報告書には次の 3 種類があります。 • SOC 1: 財務報告に係る内部統制（ICFR）に関連する可 能性がある AWS の統制環境に関する情報のほかに、ICFR の有効性の評価に関する情報を提供します。 • SOC 2: お客様および業務上の必要性があるサービスユーザーに、システムセキュリティ、可用性、および機密性に 関連するAWSの統制環境についての独立した評価を提供します。 • SOC 3: お客様および業務上の必要性があるサービスユーザーに、 AWSの統制環境についての独立した評価を提供し、AWS の内部情報を開示せずにシステムセキュリティ、 可用性、および機密性に関連する情報を提供します。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/	

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
統24	3	-	○	・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。 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。 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。 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。 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永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/	[概要] 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。 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。 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)。 [参考文献、参照URL] ○注 1 https://aws.amazon.com/jp/compliance/soc-faqs/ https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf 2 https://aws.amazon.com/jp/artifact/ https://aws.amazon.com/jp/artifact/getting-started/

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
				SOC報告書 AWS System and Organization Controls（SOC）報告書は、 AWS が重要なコンプライアンス管理および目標をどのように達成しているかを示す、独立した第三者による調査報告書です。 これらの報告書の目的は、運用およびコンプライアンスをサ ポートするために確立された AWS の統制を、お客様、および、お客様の監査人にご理解いただくことです。AWS の SOC 報告書には次の 3 種類があります。 • SOC 1: 財務報告に係る内部統制（ICFR）に関連する可 能性がある AWS の統制環境に関する情報のほかに、ICFR の有効性の評価に関する情報を提供します。 • SOC 2: お客様および業務上の必要性があるサービスユーザーに、システムセキュリティ、可用性、および機密性に 関連するAWSの統制環境についての独立した評価を提供します。 • SOC 3: お客様および業務上の必要性があるサービスユーザーに、 AWSの統制環境についての独立した評価を提供し、AWS の内部情報を開示せずにシステムセキュリティ、 可用性、および機密性に関連する情報を提供します。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24	4	-	○	・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。 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。 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。 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。	[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。 [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/

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		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永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報告書 AWS System and Organization Controls（SOC）報告書は、 AWS が重要なコンプライアンス管理および目標をどのように達成しているかを示す、独立した第三者による調査報告書です。 これらの報告書の目的は、運用およびコンプライアンスをサ ポートするために確立された AWS の統制を、お客様、および、お客様の監査人にご理解いただくことです。AWS の SOC 報告書には次の 3 種類があります。 • SOC 1: 財務報告に係る内部統制（ICFR）に関連する可 能性がある AWS の統制環境に関する情報のほかに、ICFR の有効性の評価に関する情報を提供します。 • SOC 2: お客様および業務上の必要性があるサービスユーザーに、システムセキュリティ、可用性、および機密性に 関連するAWSの統制環境についての独立した評価を提供します。 • SOC 3: お客様および業務上の必要性があるサービスユーザーに、 AWSの統制環境についての独立した評価を提供し、AWS の内部情報を開示せずにシステムセキュリティ、 可用性、および機密性に関連する情報を提供します。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24	5	-	○	・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。 AWS環境の監査、ガイドライン、リスクやコンプライ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。 https://aws.amazon.com/jp/compliance/resources/ AWS セキュリティ監査のガイドライン 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。 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 - 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確認他のサービスの 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 最新、詳細情報は下記のサイトを参照ください。 https://docs.aws.amazon.com/ja_jp/general/latest/gr/aws-security-audit-guide.html 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。 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/auditor-learning-path/	-

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
統24	6	-	○	・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。 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。 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ーの統制に関して 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、物理統制より七上の統制の監査は、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。 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永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/	-

「AWS FISC安全対策基準対応リファレンス」からの引用					参考情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
				SOC報告書 AWS System and Organization Controls（SOC）報告書は、 AWS が重要なコンプライアンス管理および目標をどのように達成しているかを示す、独立した第三者による調査報告書です。 これらの報告書の目的は、運用およびコンプライアンスをサ ポートするために確立された AWS の統制を、お客様、および、お客様の監査人にご理解いただくことです。AWS の SOC 報告書には次の 3 種類があります。 • SOC 1: 財務報告に係る内部統制（ICFR）に関連する可 能性がある AWS の統制環境に関する情報のほかに、ICFR の有効性の評価に関する情報を提供します。 • SOC 2: お客様および業務上の必要性があるサービスユーザーに、システムセキュリティ、可用性、および機密性に 関連するAWSの統制環境についての独立した評価を提供します。 • SOC 3: お客様および業務上の必要性があるサービスユーザーに、 AWSの統制環境についての独立した評価を提供し、AWS の内部情報を開示せずにシステムセキュリティ、 可用性、および機密性に関連する情報を提供します。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25	-	-	○	-	-
統26	-	-	○	-	-

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実1	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	[概要] ・暗証番号、パスワード等、利用者・システム管理者が使う秘匿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)に割当てるIAMユーザに加え、コマンドラインツール、REST API等、人以外に割当てるパスワード相当の秘匿文字列があるため注意が必要です。 ■秘匿文字列の例 ●人が対象の例 ・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 ●プログラムが対象の例 ・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、セキュリティベストプラクティス(*1)に従い設計する(後述URL参照) ・DB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やモバイルアプリのユーザ認証・認可には、Amazon Cognitoの活用も検討する: －Cognitoユーザプールは、アプリユーザのサインアップ、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フェデレーテッドアイデンティティは、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強度を上げるために、多要素認証(MFA)の設定を推奨する。 (*2)Google/Facebook/オンプレミスのActive Directory等。 [参考文献、参照URL] ・IAM 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/IAM/latest/UserGuide/best-practices.html ・AWS Systems Manager -パラメータストア 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
実2	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実3	-	○	-	[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)などを提供しています。これらのサービスの提供にあたり、AWSは取り扱うデータに関する暗号化やアクセス制御などのデータ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ができます。 [対処例] ■主な暗号化キーの管理に関する手段: AWS Key Management Service (KMS) を使用した、暗号化に用いる暗号化キーの作成および管理の方法 ・AWS KMSはカスタマーマネージドキー、AWSマネージドキー、AWS所有キーの3種類のKMSキーをサポートしています。このうち、AWSはAWSマネージドキーおよびAWS所有キーをAWS KMS上で管理します。 ■追加で選択できる暗号化キーの管理に関する手段: AWS CloudHSMを使用した、ユーザー(金融機関等)に専用に割り当てられたハードウェアセキュリティモジュール(HSM)を用いた暗号化キーの作成および管理の方法 ・AWS CloudHSMでは、バックアップやモニタリングなどの限定された操作のみをAWSが担い、暗号化キーやデータには、ユーザー(金融機関等)のみがアクセスできるよう制限されています。 ・AWS CloudHSMでは、AWSアカウントが利用するCloudHSMクラスターがFIPS140-2に準じた物理的/論理的保護の境界となります。CloudHSMクラスターより外部の保護は、AWSがVPCやIAMの機能を通じて提供する物理的/論理的保護および金融機関等が実施するVPCやIAMの設定に依存します。 [関連する認証] ・ISO/IEC 27002 -10.1 暗号による管理策 ・PCI DSS -要件3.5 カード会員データを漏洩と悪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、実装する。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報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] ・データへの適切なアクセス制御を行います。 ・有事(漏洩)の際にもデータの内容が分からないように、重要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為の各種ポリシーを利用する。例えば、IAMユーザなどデータにアクセスする側に設定する「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側に設定する「リソースベースのポリシー」がある。 ■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する。全般、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(サーバサイド暗号化)と、特定アプリのみで暗号化・復号したいケースによるクライアントサイド暗号化を選択 ・DB接続情報(認証情報)などは、Secrets ManagerやParameter Storeの利用を検討(*1)。 (*1)AWS KMSよりも厳重なキーの管理や、高いコンプライアンス要件がある場合は、AWS CloudHSMの利用も検討する。 [参考文献、参照URL] ・Amazon EC2 でのデータ保護 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 のセキュリティベストプラクティスAmazon S3 のセキュリティ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 ・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 ・AWS Systems Manager のよくある質問「Q: Secrets Manager と Parameter Store の違いは何ですか?」 https://aws.amazon.com/jp/systems-manager/faq/

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実4	-	○	-	[概要] AWSは、AWS内部のデータ通信について、取扱いに慎重を要する情報又は重要な情報を守るため、暗号化を利用しています。 [対処例] ・利用するAWSサービスがAWSマネージドなデータ伝送を行うケースにおいては、当該サービスにおける伝送経路の暗号化が、ISOまたはPCI DSSに対応していることを確認する必要があります。 ・「コンプライアンスプログラムによるAWS対象範囲内のサービス(注1)」を参照し、利用するAWSサービスがISO/PCI DSSの認証に対応しているか確認します。 [関連する認証] ・ISO/IEC 27002 -10.1 暗号による管理策 -13.2 情報の伝送 ・PCI DSS -要件4.1 オープンな公共ネットワーク経由で機密性の高いカード会員データを伝送する場合、以下のような、強力な暗号化とセキュリティプロトコルを使用して保護する。 -要件4.1.1 カード会員データを伝送する、またはカード会員データ環境に接続されているワイヤレスネットワークが、認証および伝送用に強力な暗号化を実装するため、業界のベストプラクティスを使用していることを確実にする。 [参考文献、参照URL] ○注 1　https://aws.amazon.com/jp/compliance/services-in-scope/	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報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] ・AWSの利用において、システム利用者がログインする際の経路及び開発者/運用者による維持管理の経路を暗号化します。 ・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。 [対策例] ■マネジメントコンソール及びAPIによる操作をする場合の伝送データの漏洩防止 ●伝送経路の暗号化 ・AWSマネジメントコンソール及び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。 ■各リソースへのアクセスする際の伝送データの漏洩防止 ●伝送経路の暗号化 ・HTTPSやSSH等の暗号化済のプロトコルを使って通信することも有効です。 ・Direct Connectという専用線を利用した場合でも暗号化等の漏洩防止策は必要です。 ●伝送するデータの暗号化 ・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。 [参考文献、参考URL] https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/encryption-in-transit.html
実5	-	○	-	[概要] AWSは、ファイルに対するアクセス制御を実現するためのサービスとして AWS Identity and Access Management (IAM) などを提供しています。 これらのサービスの提供にあたり、AWSはアクセス制御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、ファイルに対する適切なアクセス制御を実現することができます。 [関連する認証] ・ISO/IEC 27002 ・9.2 利用者アクセスの管理 ・9.4 システム及びアプリケーションのアクセス制御 ・PCI DSS ・要件7.1 システムコンポーネントとカード会員データへのアクセスを、業務上必要な人に限定する。 [参考文献、参照URL] ・AWS Well-Architected フレームワーク／アイデンティティ管理とアクセス管理 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/framework/a-identity-and-access-management.html	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報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] 最小権限の原則に基づき、ファイルの在処に応じてアクセス制御を行います。 [対策例] OS上のファイルやDBMS上のデータはそれぞれのレイヤのアクセス制御の仕組み(オンプレミスと同様の方法)で制御します。 AWS特有のデータ(主にAWSのリソース)は以下のようにサービス毎に用意されたアクセス制御の方法を適切に活用します。 (1)リソースベースのポリシーが設定可能なサービス(S3等) アイデンティティベースのポリシーとリソースベースのポリシーを適切に設定し、最小権限の原則に基づいた制御を行います。 ポリシー設計においては例に示すように間接的なアクセス経路についても留意が必要です。 例)例)IAMユーザーに ①Lambdaの変更許可 ②S3の閲覧拒否 のポリシーが付与されておりLambdaには ③S3の閲覧許可のポリシーを持つIAMロールがアタッチされている場合、 IAMユーザーは②によりS3を直接閲覧することはできませんが①③の組み合わせによって間接的に閲覧ができてしまいます。 (2)AWSアカウント間共有が可能なサービス(EBSスナップショット等) アイデンティティベースのポリシーにより、AWSアカウント間共有が設定できる利用者を制限します。 AWSアカウント間の共有には AWS Organizations を利用した方法が検討できます。 上記以外にも、ネットワーク的な制御で保護が可能なケースでは、セキュリティグループ等を利用して制御を行います。 不正アクセス等からのデータ保護、アクセス権限のチェック機能としては、以下のサービス群の利用(*1)が推奨されます。 (*1)参考文献「AWSご利用開始時に最低限おさえておきたい10のこと」より ・Amazon GuardDuty ： 異常なアクティビティの検出 ・AWS CloudTrail ： 操作ログの取得(イベント履歴管理) [参考文献、参照URL] https://wa.aws.amazon.com/wat.pillar.security.ja.html https://d1.awsstatic.com/webinars/jp/pdf/services/20190123_10things_at_least_for_AWSBeginner.pdf
実6	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実7	-	○	-	[概要] AWSは、すべてのAWSサービスにおいて、HTTPS通信セッションが確立可能な、安全なAPIエンドポイントを提供しています。伝送中のデータを保護するために、TLSがサポートされています。また、AWSは伝送中のデータを保護するための対策に係る認証を取得しています。 [関連する認証] ・ISO/IEC 27001 -10.1 暗号による管理策 -13.2 情報の転送 ・PCI DSS -要件4 オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する [参考文献、参照URL] ・セキュリティの柱　AWS Well-Architected フレームワーク／伝送中のデータの保護 https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/protecting-data-in-transit.html	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報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] 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須となります。 [対策例] ■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が備え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の利用を選択するサービス(例：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は利用者の責任でTLSの設定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密鍵の保護を目的に、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機能により、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記述します。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、ツールの設定で指定したアクセスキーにより自動で署名されます。 ■特定システムなど安全対策の水準を高める要件がある場合には、業務データへ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実装において AWS KMS APIなどを使用し、クライアントのリクエストにより業務データへの電子署名を行い、伝送経路を通じたデータ(署名データを含む)のやり取りの後、サーバ側でデータの署名検証を行います。 [参考文献、参照URL] ・Application Load Balancer 用の HTTPS リスナーを作成する https://docs.aws.amazon.com/ja_jp/elasticloadbalancing/latest/application/create-https-listener.html ・AWS Certificate Manager ユーザーガイド https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html ・AWS CloudHSM で SSL/TLS オフロードでウェブサーバーのセキュリティを向上させる https://docs.aws.amazon.com/ja_jp/cloudhsm/latest/userguide/ssl-offload.html ・AWS API リクエストへの署名 https://docs.aws.amazon.com/ja_jp/general/latest/gr/signing_aws_api_requests.html ・AWS KMS の新機能 公開鍵暗号によるデジタル署名 https://aws.amazon.com/jp/blogs/news/digital-signing-asymmetric-keys-aws-kms/
実8	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	[概要] AWS特有の本人確認が必要となるケースとして、AWSレイヤのユーザ(ルートユーザ、IAMユーザ)の利用があります。 AWSレイヤのユーザの認証で確実な本人確認を行うための対策を検討・実装します。 また、アプリケーションレイヤのユーザの管理にAWSのサービス(例：Amazon Cognito)を利用する場合には、当該ユーザに対しても対策を検討・実装します。 [対策例] [概要]に記載したユーザの不正アクセス防止に対する有効な対策例として、パスワードだけでなく追加の認証情報を必須とする多要素認証機能(※１)(※２)や、ログイン元IPアドレスに応じた権限制御の機能(※３)を利用することが挙げられます。 なお、OS以上のレイヤでかつAWSの機能を利用せずに管理するユーザに対して施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。 [参考文献、参照URL] (※１)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 (※２)Amazon Cognito デベロッパーガイド ・ユーザープールへの多要素認証 (MFA) の追加 https://docs.aws.amazon.com/ja_jp/cognito/latest/developerguide/user-pool-settings-mfa.html (※３)AWS Identity and Access Managementユーザーガイド ・AWS: 送信元 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
実9	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	[概要] AWS利用に伴い追加で保護対象となるIDとして、AWSレイヤのユーザ(ルートユーザ、IAMユーザ)があります。 AWSレイヤのユーザのIDの不正使用を防止するための対策を検討・実装します。 また、アプリケーションレイヤのユーザの管理にAWSのサービス(例：Amazon Cognito)を利用する場合には、当該ユーザに対しても対策を検討・実装します。 [対策例] 本基準に記載されているIDの不正使用防止機能の例に対して、AWSでは対応する機能(下記)が提供されています。 なお、OS以上のレイヤでかつAWSの機能を利用せずに管理するユーザに対して施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。 ・マネジメントコンソールでは、ログイン後12時間で自動ログアウトするようになっています。(※１) ・IAMロールを利用することで、プログラム等に ID・パスワードを直接記述することなく、AWSリソースにアクセスすることが可能です。(※２) ・正当な権限を持たない第三者によるIDの不正使用対策として、AWSでは多要素認証や接続元IPアドレス制限等の実装が可能です。(※３)(※４)

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
						[参考文献、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: 送信元 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 ユーザープール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
実10	-	○	- -	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	[概要] AWS利用に伴い、追加でアクセス履歴の取得・保管・監査対象となるものとして、下記があります。 アクセス履歴取得・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履歴 ・AWSリソースに対するアクセス履歴 (例：Amazon S3・Amazon RDS等のデータへのアクセス履歴、ELBへのアクセス履歴) [対策例] AWSリソース自体の操作履歴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の実行履歴を出力・保管することができ、当該情報を監査証跡として活用可能です。(※1) AWSリソースに対するアクセス履歴は、各サービスで提供されているインターフェースにより収集・保管可能です。 (一部サービスの例を(※2)(※3)(※4)に示します。) なお、OS以上のレイヤで施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牽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。 [参考文献、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/awscloudtrail/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操作 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
実11	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実12	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実13	-	○	-	[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)等を提供しています。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上において、プリンシパルと呼称されます)に対してのみ、その暗号化キーの利用を制限することができます。これらのサービスの提供にあたり、AWSは取り扱うデータに関する暗号化やアクセス制御などのデータ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とすることができます。 [対処例] ■主な暗号化キーの管理に関する手段: AWS Key Management Service (KMS) を使用した、暗号化に用いる暗号化キーの作成および管理の方法 ・AWS KMSはカスタマーマネージドキー、AWSマネージドキー、AWS所有キーの3種類のKMSキーをサポートしています。このうち、AWSはAWSマネージドキーおよびAWS所有キーをAWS KMS上で管理します。 ■追加で選択できる暗号化キーの管理に関する手段: AWS CloudHSMを使用した、ユーザー(金融機関等)に専用に割り当てられたハードウェアセキュリティモジュール(HSM)を用いた暗号化キーの作成および管理の方法 ・AWS CloudHSMでは、バックアップやモニタリングなどの限定された操作のみをAWSが担い、暗号化キーやデータには、ユーザー(金融機関等)のみがアクセスできるよう制限されています。また、AWS CloudHSMには、物理的および論理的な不正使用を検知して保護する仕組みが搭載されています。さらに、暗号化キーの生成時に仕様する乱数源も、高品質な真性乱数ジェネレーター(TRNG)が搭載されています。これらの仕様により、AWS CloudHSMを用いることで、ユーザー(金融機関等)は、よりセキュアな暗号化キーの管理を行うことが可能です。	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。	[概要] ・暗号鍵を安全に管理します。 [対策例] ・要件に応じ、下記サービスを検討する (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準拠が必要といった、高いコンプライアンス対応の為のサービス。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御、詳細は参考文献)。必要に応じ、IAMポリシー(使う側)でのアクセス制御を設定する事もできます(*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となる [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

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
				[関連する認証] ・ISO/IEC 27001 -10.1 暗号による管理策 ・PCI DSS -要件3.5 カード会員データを漏洩と悪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、実装する。 [参考文献、参照URL] ・AWS Key Management Service のよくある質問 https://aws.amazon.com/jp/kms/faqs/		
実14	○	○	・AWSネットワークは、従来のネットワークセキュリティ問題に対する強力な保護機能を提供します。 保護機能の例： - 分散サービス拒否（DDoS）攻撃 - 中間者（MITM）による攻撃 - IPスプーフィング - ポートスキャン - 第三者によるパケットスニッフィング AWS は、様々な自動モニタリングシステムを活用して、ハイレベルなサービスパフォーマンスと可用性を提供します。AWS モニタリングツールは、異常な、または不正なアクティビティと条件を通信の出入り口で検出するように設計されています。これらのツールは、サーバーおよびネットワークの利用状況、ポートスキャニングアクティビティ、アプリケーションの利用状況、および許可されていない侵入の試みをモニタリングします。 モニタリングに加えて、AWS 環境内のホストオペレーティングシステム、ウェブアプリケーション、およびデータベースで様々なツールを使用した脆弱性のスキャンが定期的に実行されます。また、AWS セキュリティチームは、該当するベンダーの不具合に関するニュースフィードを購読し、積極的にベンダーのウェブサイトやその他の関連する販売経路を監視し、新しいパッチがないかどうかの確認を行っています。さらに、AWS のお客様から各種問題を AWS にご報告いただけるようにしています。AWS 脆弱性レポートのウェブサイト（http://aws.amazon.com/security/vulnerability-reporting/）をご利用ください。	[概要] AWSの各種サービスはAWS データセンターで稼働します。 AWSは、AWS データセンターにおける外部ネットワークからの侵入防止に係る認証を取得しています。 [関連する認証] ・ISO/IEC 27001 - 12.2 マルウェアからの保護 - 12.4 ログ取得及び監視 ・PCI DSS - 10.2 次のイベントを再現するために、すべてのシステムコンポーネントの自動監査証跡を実装する。 - 10.6 すべてのシステムコンポーネントのログとセキュリティイベントを調べ、異常や怪しい活動を特定する。 - 11.4 侵入検知システムや侵入防止手法を使用して、ネットワークへの侵入を検知および/または防止する。 [参考文献、参照URL] ・AWS データセンターのセキュアな設計について解説します。 https://aws.amazon.com/jp/compliance/data-center/	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 インフラストラクチャ保護: Amazon Virtual Private Cloud (Amazon VPC) を使用して、お客様が定義した仮想ネットワーク内で AWS リソースを起動できます。Amazon CloudFront は、DDoS を緩和する AWS Shield に統合されたビューワーに対して、データ、動画、アプリケーション、API を安全に提供する、グローバルコンテンツ配信ネットワークです。AWS WAF は、ウェブの一般的な脆弱性からウェブアプリケーションを保護するために役立つ、Amazon CloudFront または Application Load Balancer にデプロイされたウェブアプリケーションファイアウォールです。	[概要] システムで保護すべき情報資産に応じて、多層的に外部ネットワークからの不正侵入防止策を講じます。 [対策例] ■対象システムに紐づくアカウント群のAWSマネジメントコンソールおよびAPIアクセスにおける防止策例 ・ルートユーザおよびIAMユーザにおいて、二要素認証を有効化します。 ・IAMアクセスキーの漏洩が発生しないように git-secrets を利用します。 ・IAMユーザー/グループにおいて接続先IPアドレスによる制限を行うIAMポリシーを付与します。 → ルートユーザではIAMポリシーによる制御を行えない点に留意します。 （注)ルートユーザについてはAWS Organizationsのサービスコントロールポリシーで制御します。 ・Amazon GuardDutyの有効化により、通常のパターンとは異なる接続元からサインインされた場合に検知できるようにします。 ■対象システムを構成するAWSリソースにおける防止策例（「お客様が統制すべき内容」に記載されていないもの） ・VPCにおいてプライベートサブネットとパブリックサブネットを分離し、EC2やRDSへのパブリックアクセスを許可しないようにします。 ・外部への機密情報の流出防止等を目的として、VPC内部からVPC外部の通信はすべてプロキシサーバを経由するようにします。 → セキュリティグループではIPアドレスやプロトコルによる制御にとどまるため、URLフィルタにはプロキシを利用する必要があります。 ・EC2インスタンスにおけるOSの脆弱性対策を行います。 → Amazon Inspectorが対応するOSであれば、Inspectorの利用により検出が可能です。 ・AWS WAFやAWS Shieldを利用して不正アクセスを検知・防御します。 → WAF Managed Rules は提供者により自動でルールがアップデートされます。 → 誤検知や誤遮断を防止するためにCountモードでのWAFログ分析後にBlockモードへ移行することが推奨されます。 ・アンチウイルスやIDS/IPSの導入、侵入検知などサードパーティソリューションを利用します。 [参考文献、参照URL] https://wa.aws.amazon.com/wat.pillar.security.ja.html https://github.com/awslabs/git-secrets
実15	○	○	・AWS では、インバウンドとアウトバウンドの通信およびネットワークトラフィックをより包括的に監視することを考え、限られた数のクラウドへのアクセスポイントを戦略的に設置しました。このようなお客様のアクセスポイントは API エンドポイントと呼ばれ、安全な HTTP アクセス（HTTPS）を許可します。これにより、ご利用のストレージまたは AWS 内のコンピューティングインスタンスとの安全な通信セッションを確立できます。FIPS 暗号要件への準拠を必要とするお客様をサポートするために、AWS GovCloud（米国）内の SSL 終端ロードバランサーは、FIPS 140-2 に準拠しています。 さらに、AWS は、インターネットサービスプロバイダ（ISP）とのインターフェイス通信を管理するためのネットワークデバイスを実装しました。AWS ネットワークのインターネット側のそれぞれの境界では、複数の通信サービスへの重複する接続を採用しています。これらの接続にはそれぞれ、専用ネットワークデバイスがあります。 追加情報については、"アマゾン ウェブ サービス: セキュリティプロセスの概要"を参照してください。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 お客様はAmazon VPCを使用することにより、アマゾン ウェブ サービス (AWS) クラウド内で論理的に分離したセクションをプロビジョニングし、お客様が定義する仮想ネットワークで AWS リソースを起動できます。また、VPC 内のセキュリティグループにより、各 Amazon EC2 インスタンスにおける着信および発信両方のネットワークトラフィックを指定することができます。明示的に許可されていないトラフィックは自動的に拒否されます。 セキュリティグループに加えて、各サブネットに出入りするネットワークトラフィックは、ネットワークアクセスコントロールリスト (ACL) を使用して許可または拒否することができます。 AWS PrivateLink を使用して、VPC と AWS のサービスをセキュアでスケーラブルな方法で接続できます。AWS PrivateLink のトラフィックはインターネットを経由しないため、ブルートフォース攻撃や DDoS (分散型サービス拒否) 攻撃の脅威に晒される危険を軽減できます。プライベート IP 接続とセキュリティグループを使用することで、サービスは自社のプライベートネットワークで直接ホストしているように機能します。	[概要] ・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。 [対策例] ■外部(マネジメントコンソール及びAPIの操作)からのアクセス制御 ●IAMポリシーによる制御 ・IAMユーザーに対し、アクセス元のIPアドレスを制限するIAMポリシーを適用します。 ■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の外に配備するリソース(代表例：S3バケット)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。 ・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に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少させることも有効です。 ●利用者側の設定による制御(クラウド利用に限らない従来の制御) ・FW等の設定において、IPアドレスのアクセス制限の設定を行います。 ・アクセス用の端末やアクセス経路上の端末に不必要なソフトウェアはインストールしないようにします。

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実16	○	○	AWS は AWS システム内でシステムとデバイス間で監査可能なイベントカテゴリを識別しています。サービスチームは監査機能を設定して、要件に従って継続的にセキュリティ関連イベントを記録しています。ログストレージシステムは、ログストレージの次のニーズが発生すると自動的に容量を増やす、スケーラブルで高可用性のサービスを提供するように設計されています。監査記録には、必要な分析要件をサポートするために、データ要素のセットが含まれます。さらに AWS セキュリティチームまたはその他の適切なチームは、要求時に検査または分析を実行するため、またはセキュリティ関連のイベントやビジネスに影響するイベントに応じて、監査記録を使用できます。 AWS チームの指定された関係者は、監査処理が失敗した場合に、自動化されたアラートを受け取ります。監査処理の失敗には、ソフトウェアハードウェアのエラーなどが含まれます。オンコール担当者は、アラートを受け取るとトラブルチケットを発行し、解決されるまでイベントを追跡します。 AWS のログおよびモニタリングプロセスは、SOC、PCI DSS、ISO/IEC 27001、および FedRAMPsm コンプライアンスへの AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 AWS Shield は、AWS で実行されるアプリケーションを Distributed Denial of Service (DDoS) 攻撃から保護するマネージド型のサービスです。AWS Shield Standard は、すべてのお客様に対し追加料金なしで自動的に有効化されます。AWS Shield Advanced は任意で利用できる有料サービスです。AWS Shield Advanced により、Amazon EC2、Elastic Load Balancing (ELB)、Amazon CloudFront、AWS Global Accelerator、Route 53 で実行中のアプリケーションを標的とする、高度化された大規模な攻撃からの保護を強化することができます。 また、Amazon GuardDuty は、AWS アカウントとワークロードを継続的にモニタリングおよび保護できる脅威検出機能を提供しています。お客様はGuardDuty を使用することで、AWS CloudTrail イベント、Amazon VPC フローログ、および DNS ログで見つかったアカウントとネットワークアクティビティから生成されたメタデータの連続ストリームを分析することができます。また、既知の悪意のある IP アドレス、異常の検出、機械学習などの統合された脅威インテリジェンスを使用して、脅威をより正確に識別することができます。	[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攻撃の踏台にされている等)。 [対策例] ・Amazon GuardDuty(*1)を有効にする。全リージョンでの有効化が推奨。 ・リアルタイムな検知が必要であれば、CloudWatch Eventsなど利用し、通知を行う。 ・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。 (*1)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独立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は有効にしなくても利用できます(後述、よくある質問参照)。但し、これらのログは、有事の際のトラブルシュートや、監査に利用されるため、有効化の上、適切な保存が必要なケースが殆どです。 例)CloudTrailの有効化と、証跡ログの保存・保護等。 [参考文献、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-guarduty-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?両方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/
実17	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実18	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実19	○	○	Amazon のインシデント管理チームは、業界標準の診断手順を採用しており、事業に影響を与えるイベント時に解決へと導きます。作業員スタッフが、24 時間 365 日体制でインシデントを検出し、影響と解決方法を管理します。AWS の事故対応プログラム、計画、および手続きは、ISO/IEC 27001 の認証基準に合わせて作成されています。AWS SOC 1 Type 2 レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。 詳細については、"アマゾン ウェブ サービス : セキュリティプロセスの概要"ホワイトペーパー (http://aws.amazon.com/security) を参照してください。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 お客様はAmazon Detective を使用することにより、潜在的なセキュリティ問題や不審なアクティビティの根本原因を簡単に分析、調査し、すばやく特定できます。Amazon Detective は、AWS リソースからログデータを自動的に収集し、機械学習、統計的分析、グラフ理論を使用して、リンクされたデータセットを構築します。これにより、より迅速かつ効率的なセキュリティ調査を簡単に行えます。	[概要] 不正アクセスについては(1)アカウントへ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、それぞれのレイヤで対策が必要です。また、不正アクセスの証跡を確保し、インシデント発生後に原因と被害範囲の調査が出来るよう予め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抑止するため、(3)マルチアカウント利用時の推奨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の有効化、GuardDutyの有効化、Amazon Detectiveの有効化。 ・証跡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 復旧に際しては漏えいした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。 ・証跡ログを確認し、改ざん箇所の特定を行い、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活用する。 ・Amazon Detectiveによる脅威調査と、GuardDuty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の特権的アクセスを奪取されるケースにおいては権限管理の徹底と、アクセス経路の限定が有効です。 ・ 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、都度ID,パスワードを払い出す体制とする。 ・ Systems Manager Session Managerを利用し、IAMへのアクセス権限を集約し、MFAの有効化を行う。 ・ 踏み台環境を用意し、アクセス経路を限定する(ex. セキュリティグループによる送信元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、ログ証跡保管(証跡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当該システムまでのアクセス経路に置くゲートウェイ型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、証跡の確保と、悪意あるアクセスの遮断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内の通信経路におけるロギング - Route 53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サーバログの取得(ELBログの場合はHttpヘッダのx-fowording-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 FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
						不正アクセスの原因究明・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上の設定パラメータ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。 復旧に関しては、予めEBS Snapshotを定期的に取得しておくことが重要です。 また、各AWSマネージドサービスを復旧は構築時のパラメータシートを元に手作業での復旧することも可能ですが、より迅速、確実に復旧するため、AWS CloudFormation、AWS OpsWorks、AWS CodePipelineなどを利用し、各AWSマネージドサービスおよびアプリケーションを再構築する冪等性の高いパイプラインやスクリプトを用意するとより確実かつ迅速な復旧が可能です。 再発防止対策は下記の通りです。 ・Amazon Inspectorによるセキュリティ評価 ・Amazon GuardDutyの有効化による脅威検知 ・その他サードパーティが提供する脆弱性検査サービスの利用 (3) マルチアカウント利用時の推奨対策 多数のアカウントを利用している環境においてはログの分散と設定ミスによるAWS CloudtrailやAWS Configによる証跡ログの取り忘れ、改ざんが生じる可能性があります。これを抑制するには、証跡ログを一か所に集める集中管理型のアカウントの利用が推奨されます。 ・セキュリティ＆監査用集中管理型のアカウントを別に用意。 ・各アカウントのCloudTrailログ出力先を全て上記アカウントに指定 ・上記アカウントに対しては通常のアドミニストレータによるアクセスは許可せず、 セキュリティ調査、監査に関わるスタッフのみ許可する。 ・上記アカウント上のログはAmazon KMSを利用し暗号化を行う ・AWS Organizationsを利用し、AWS CloudTrailを強制的に全アカウントへ適用する。 また、マルチアカウント環境においては多数のアカウント個別でIAMユーザを持つと管理が煩雑となり、不適切な権限の適用や、ユーザの消し忘れに起因したなりすましの温床となるため、集中的にIAMユーザを管理するアカウントを用意、実際に利用するアカウントに対してはIAMロールによるクロスアカウントアクセスを行うことで、ユーザ管理の負荷を軽減することができます。 [参考文献、参考URL] https://aws.amazon.com/jp/whitepapers/overview-of-security-processes/ https://d1.awsstatic.com/International/ja_JP/Whitepapers/AWS_Security_Best_Practices.pdf
実20	-	○	-	[概要] AWSは、ウイルス対策および悪意のあるソフトウェア対策への防御対策を実施しています。また、アマゾン ウェブ サービスには、Amazon RDS、Amazon ECS、AWS Fargate 等のAWS マネージド型サービスについてウイルス対策およびマルウェア対策ソリューションのデプロイおよび管理を行う責任があります。AWSは、ウイルス対策および悪意のあるソフトウェア対策への防御対策に係る認証を取得しています。 [関連する認証] ・ISO/IEC 27001 - 12.2 マルウェアからの保護 ・PCI DSS - 要件 5 マルウェアにしてすべてのシステムを保護し、ウィルス対策ソフトウェアを定期的に更新する。 [参考文献、参照URL] ・AWS における PCI DSS (Payment Card Industry Data Security Standard) 3.2.1 コンプライアンスガイド https://d1.awsstatic.com/whitepapers/ja_JP/compliance/pci-dss-compliance-on-aws.pdf ・CSA_Consensus_Assessments_Initiative_Questionnaire https://d1.awsstatic.com/whitepapers/compliance/CSA_Consensus_Assessments_Initiative_Questionnaire.pdf ・脆弱性情報の収集 https://aws.amazon.com/jp/security/vulnerability-reporting/	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報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] コンピュータウイルス等の不正プログラムへの防御対策を講ずる必要があります。 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。 [対策例] EC2 インスタンス上の基盤となるオペレーティングシステムに対しては、お客様にて適切なウイルス対策ソフトウェアや改ざん検出ソフトウェアを構成して実行する責任があります。 AWS Marketplaceでは、お客様が利用する多数のウイルス対策、マルウェア対策並びに改ざん検出ソリューションを提供しているため、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。AWS Marketplaceから購入したソフトウェア・マシンイメージの本番適用前には試験用の環境等を用いて、正当性や動作等の検証を行ったうえで導入することを推奨します。 尚、Amazon RDS、Amazon ECS、AWS Fargate等の AWS マネージド型サービスについては、AWSにウイルス対策およびマルウェア対策ソリューションのデプロイおよび管理を行う責任があります。
実21	○	○	ウイルス対策および悪意のあるソフトウェア対策に関する AWS のプログラム、プロセス、および手続きは、ISO/IEC 27001 に準拠しています。 詳細についてはISO/IEC 27001 の附属書 A、ドメイン 12 を参照してください。AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 また、Amazon の資産 (ノートパソコンなど) は、E メールのフィルタリングとマルウェア検出を含むウイルス対策ソフトウェアで設定されています。 AWS ネットワークファイアウォール管理および Amazon のウイルス対策プログラムは、SOC、PCI DSS、ISO/IEC 27001、および FedRAMPsm への AWS の継続的な準拠の一環として、第三者の独立監査人によって確認されます。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	[概要] コンピュータウイルス等の不正プログラムの検知対策を講じる必要があります。システムの信頼性を確保・維持するため、コンピュータウイルス等の不正プログラムの侵入及び組込みの有無を検証する検知対策を講じる必要があります。 一般的なEC2等のサービスインスタンスへの対策であれば、オンプレミスと同等の考え方で、アンチウイルスソフトウェアを使用した対策を講じる事となります。一方、コンテナやクラウドストレージ等のクラウド特有のサーバレスサービスを使用してシステムを構築する場合、一般的なアンチウイルスソフトウェアを導入できない場合があるため、それぞれのサービスに適応した対策が必要となります。また、一般的なアンチウイルスソフトウェアは既知のウイルスに対する防御機能が実装されている場合が多く、新種ウイルスのような未知のウイルスに対する防御は難しいため、不正侵入されることを前提としたシステム稼働ログ分析機能等による早期検知・対応対策の導入についても検討が必要です。ネットワーク通信の監視、API状態の監視、プロセス振舞い監視等の各監視ログを相関分析することにより、システムの不審な挙動を検知する対策となります。 [対策例] ■ウイルス対策の例 ・アンチウイルス対策ソフトウェアの導入 ■早期検知・対応策の例 ・AWSのセキュリティサービスの利用 -AWS Security Hub の特徴(※1) -Amazon GuardDuty の特徴(※2) ■セキュリティ対策ソフトウェアによる対応 ・サービスインスタンスへのEndpoint Detection & Response(EDR)ソリューション等の導入 [参考文献、参照URL] (※1)https://aws.amazon.com/jp/security-hub/features/ (※2)https://aws.amazon.com/jp/guardduty/features/

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実22	○	○	AWS の事故対応プログラム、計画、および手続きは、ISO/IEC 27001 に準拠して作成されています。AWS SOC 1 Type 2 レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	[概要] コンピュータウイルスの感染を検知または発病、あるいは不正プログラムを発見した場合などに備え、対応手順を整備しておくことが重要です。 [対策例] コンピュータウイルスの感染を検知または発病、あるいは不正プログラムを発見した場合などAWSを利用した対応手順としては下記が考えられます。 ・感染システムの切り離し 切り離し方法として、ネットワークACL/セキュリティグループ等での通信の切断、AWSマネジメントコンソールからのシステムの停止などがあります。 (注)EC2インスタンスを停止する場合、メモリ内の情報などが消去されるため、痕跡が消える場合があります。フォレンジック調査を行う場合は、EC2インスタンスの停止前に通信の切断を行ったうえで必要なデータ取得を行う必要があります。これ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。 ・バックアップからの復旧 バックアップの取得方法として、ボリュームやインスタンスのSnapShot、AMI取得などがあります。 コンピュータウィルス感染による被害を特定するために、外部との通信経路の制限や把握が有効となります。プロキシサーバを設置し、通信先を制限することにより感染後の2次被害を防げる可能性があります。直接インターネットと通信する場合は、どのサービスがインターネットへ通信しているか把握しておく必要があります。
実23	○	○	AWS セキュリティフレームワークは、NIST SP800-53、ISO/IEC 27001、ISO/IEC 27017、ISO/IEC 27018、ISO 9001 基準、および PCI DSS 要件に基づいて、ポリシーと手続きを規定しています。 詳細につい ては 、アマゾン ウェブ サービス ：リスクとコンプライアンスホワイトペーパー を参照してください。 AWS には、毎年（またはポリシーに影響するシステムへの大きな変更が発生したときに）確認、更新される正式なアクセスコントロールポリシーがあります。このポリシーでは、目的、範囲、役割、責任、および管理コミットメントについて取り上げています。AWS は最小権限という概念を導入しており、ユーザーがジョブ機能を実行するために必要最小限のアクセスを許可しています。ユーザーアカウントの作成では、最小アクセス権を持つユーザーアカウントが作成されます。これらの最小権限を超えるアクセスには、適切な認証が必要になります。詳細情報については、ISO/IEC 27001 基準および 27018 行動規範を参照してください。AWS は独立監査人により ISO/IEC 27001 および ISO/IEC 27018 に準拠している旨の審査と認定を受けています。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	[概要] AWSのサービスに対する操作を含むマニュアルについて、以下に留意して作成します。 ・AWSサービス/機能への追随 ・マネジメントコンソールにおける日々のUIの改善 ・キャプチャを多用する場合、保守性の観点で最新化維持の負荷を考慮 また、サービスや機能の仕様変更に応じてマニュアルの見直しが必要となる場合があります。そのため、定期的なマニュアルの見直しやマニュアルの実機訓練の検討が必要です。 [対策例] ・マネジメントコンソール等を使ったオペレーションマニュアル ・AWSシステムメンテナンス時の対応マニュアル 保守性の観点で以下を考慮して作成することも有効です。 ・AWS CLIや各プログラミング言語(AWS CloudFormationやAWS CDK等)からの操作を検討 ・手順書作成を自動化する効率化ツールを採用 [参考文献、参照URL] ・AWS Artifact https://aws.amazon.com/jp/artifact/
実24	○	○	AWS のビジネス継続性ポリシーおよび計画は、ISO/IEC 27001 に準拠して開発され、テストされています。AWS とビジネス継続性の詳細については、ISO/IEC 27001 の附属書 A、ドメイン 17を参照してください。 詳細については 、アマゾン ウェブ サービス ：リスクとコンプライアンス ホワイトペーパー を参照してください。 AWS マネジメントは、リスクを緩和または管理するためのリスク特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、戦略的事業計画を再評価します。このプロセスでは、マネジメントがその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実25	○	○	AWS は、ISO/IEC 27001 に準拠して、AWS リソースに対する論理アクセスについて最小限の基準を示す正規のポリシー、手続きを規定しています。AWS SOC レポートには、AWS リソースに対するアクセスプロビジョニングを管理するために用意されている統制の概要が記載されています。 詳細については 、アマゾン ウェブ サービス ：リスクとコンプライアンス ホワイトペーパー を参照してください。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 お客様はAWS Identity and access Management(IAM) を使用して、お客様の AWS リソースへの個人またはグループによるアクセスを安全にコントロールすることができます。 お客様はCloudTrail を使用することで、リクエストを実行したユーザー、使用したサービス、実行されたアクション、そのアクションのパラメーター、AWS のサービスによって返されたレスポンス要素など、各アクションの重要な情報が記録することができます。この情報は、AWS リソースに加えられた変更を追跡し、操作に関する問題を解決するために役立ちます。	[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を特定し、アクセス権限所有者が必要最小限となるよう制御する必要があります。 [対策例] 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追加することにより、AWSリソース側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のカスタマー管理型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

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実26	○	○	AWSではISO/IEC 27001およびPCI DSSに則り、AWSリソースへの論理的なアクセスのために必要なパスワードポリシーを定めています。パスワードは複雑である必要があり、90 日おきに変更されます。 AWS環境におけるパスワード要件の詳細については、PCI DSS レポート 8.2 および SOC2 タイプ2レポートを参照ください。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 お客様はAWS Identity and access Management(IAM) を使用して、お客様の AWS リソースへの個人またはグループによるアクセスを安全にコントロールすることができます。AWS IAMでは、パスワードの最小長を定義したり、数字を 1 つ以上含めるようにするなど、強力なパスワードを要求できます。自動パスワード失効の実施、以前に使用したパスワードの再利用禁止、次回 AWS サインイン時のパスワードリセットの要求も設定できます。	-
実27	○	○	AWS 本稼働環境のネットワークは、Amazon 社内ネットワークから分離されており、論理的アクセスのために個別の認証情報が必要です。 AWS クラウドのコンポーネントにアクセスする必要がある Amazon 社内ネットワーク上の AWS 開発者と管理者は、AWS アクセス管理システムを通して明示的にアクセスをリクエストしなければなりません。すべてのリクエストは、適切な所有者または管理者によって確認および承認されます。 アカウントの確認および監査 アカウントは 90 日ごとにレビューされます。明示的な再承認が必要となり、これを行わない場合は、リソースに対するアクセス権が自動的に取り消されます。従業員の記録が Amazon のヒューマンリソースシステムから削除されると、アクセス権は自動的に取り消されます。Windows および UNIX のアカウントは無効となり、Amazon の権限管理システムは全システムからそのユーザーを削除します。 アクセスに関する変更リクエストは、Amazon 権限管理ツールの監査ログに記録されます。従業員の役職に変化が生じる場合、リソースに対するアクセスの継続が明示的に承認される必要があります。承認しない場合、アクセス権は自動的に取り消されます。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
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。	[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、データファイルの授受・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。 [対策例] 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 ボリュームとスナップショットを AES-256 で暗号化する機能があり、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リクエストヘッダーを単純に追加するだけで、アップロード時にデータを暗号化することができます。データが取得された時に、自動的に復号が行われます。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 メタデータに機密情報を含めないことをお勧めします。
実29	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実30	-	○	-	[概要] 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、策定した手続きを実現するための機能がAWS上に存在するかを確かめる必要があります。 [関連する認証] ・ISO/IEC 27001 -10.1 暗号による管理策 ・PCI DSS -要件3.5 カード会員データを漏洩と誤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。 -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、実装する。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報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31	○	○	新たに採用した従業員には体系的な入社時研修を行い、Amazon のツール、プロセス、システム、ポリシー、手順について熟知させます。 ISO/IEC 27001 に準拠して、すべての AWS 従業員は、修了時に承認を必須とする定期的な情報セキュリティトレーニングを修了しています。従業員が制定されたポリシーを理解し遵守していることを確認するために、コンプライアンス監査を定期的に実施しています。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実32	○	○	ウイルス対策および悪意のあるソフトウェア対策に関する AWS のプログラム、プロセス、および手続きは、ISO/IEC 27001に準拠しています。詳細については、AWS SOC レポートを参照してください。 また、詳細については、ISO/IEC 27001 の附属書 A、ドメイン 12 を参照してください。AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 また、Amazon の資産 (ノートパソコンなど) は、E メールのフィルタリングとマルウェア検出を含むウイルス対策ソフトウェアで設定されています。 AWS ネットワークファイアウォール管理および Amazon のウイルス対策プログラムは、SOC、PCI DSS、ISO/IEC 27001、および FedRAMPsm への AWS の継続的な準拠の一環として、第三者の独立監査人によって確認されます。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	[概要] ウイルス対策に関しては、オンプレミスと同様に導入された技術的防御対策の管理・保守の手順を明確にする必要があります。 加えて検知・復旧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。 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。 また、クラウド事業者責任範囲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。
実33	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実34	○	○	AWS ネットワーク管理は、SOC、PCI DSS、ISO/IEC 27001、および FedRAMPsm への AWS の継続的な準拠の一環として、第三者の独立監査人によって定期的に確認されます。 ネットワークの監視と保護 AWS は、様々な自動モニタリングシステムを活用して、ハイレベルなサービスパフォーマンスと可用性を提供します。AWS モニタリングツールは、異常な、または不正なアクティビティと条件を通信の出入り口で検出するように設計されています。これらのツールは、サーバーおよびネットワークの利用状況、ポートスキャニングアクティビティ、アプリケーションの利用状況、および許可されていない侵入の試みをモニタリングします。このツールを使用して、異常なアクティビティに対して独自に性能測定基準のしきい値を設定することができます。 AWS 内のシステムには膨大な装置が備わっており、主要なオペレーションメトリックをモニタリングしています。主要なオペレーションメトリックが早期警告しきい値を超えた場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。オンコールスケジュール（常時待機体制）が採用されているので、担当者が運用上の問題にいつでも対応することができます。ポケットベルシステムがサポートされ、アラームが迅速かつ確実に運用担当者に届きます。 AWS 環境内のホストオペレーティングシステム、ウェブアプリケーション、およびデータベースで様々なツールを使用した脆弱性のスキャンが定期的に実行されます。また、AWS セキュリティチームは、該当するベンダーの不具合に関するニュースフィードを購読し、積極的にベンダーのウェブサイトやその他の関連する販売経路を監視し、新しいパッチがないかどうかの確認を行っています。	[概要] AWS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について説明しています。また、外部接続における運用管理に関する対策に係る認証を取得しています。 [対処例] ・サードパーティのアクセスは、AWS 従業員であっても、データセンターへのアクセスを厳密に統制しています。第三者による AWS データセンターへのアクセスは、AWS アクセスポリシーに従って適切な AWS データセンターマネージャーによって明示的に許可されない限り、実施されません。 ・内部者によるアクセスは、AWS は、内部者による不適切なアクセスの脅威に対処するために特定の SOC 1 統制を規定しています。 ・定期的なリスク評価時に、内部者によるアクセスの統制および監視方法を評価しています。 ・AWS では、システムを 24 時間体制でモニタリングしている世界トップクラスのセキュリティ専門家チームがおり、お客様のコンテンツを保護しています。データセンターとリージョンを相互接続する AWS グローバルネットワークを流れるすべてのデータは、安全性が保証された施設を離れる前に物理レイヤーで自動的に暗号化されます。 [関連する認証] ・ISO/IEC 27001 -13.1 ネットワークセキュリティ管理 -14.1 情報システムのセキュリティ要求事項 [参考文献、参照URL] ・AWS クラウドセキュリティ https://aws.amazon.com/jp/security/ ・主要なコンプライアンスに関する質問と AWS の回答 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Answers_to_Key_Compliance_Questions_JP.pdf	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報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] 外部接続における運用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は、AWSが提供する機能および情報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、AWS Trusted Advisor (※1)を提供しており、お客様がセキュリティチェック を使用することでセキュリティ対策や監視を強化することが出来ます。 [対策例] (1) 接続先の確認、制限 ① 接続する際は相手の本人確認、端末確認を行う。確認方法は【実2、実8】を参照。 ② 確認に使用するパスワード等の登録・変更は定められた方法によって行い、その結果については確認検証を行う。管理方法は【実1、実26】を参照。 (2) 外部接続の利用管理 社内システムとインターネットとの接続や、出張先からのリモートアクセス等を行う場合は、① 利用可能者、② 利用可能時間、③ 利用目的の３点を定め、場合によっては制限を設ける。 (3) 接続の監視 不正アクセスや情報漏洩防止のため、接続記録を取得し以下の監視を行う。 監視方法は【実10、実16】を参照。 ① 外部から内部への接続監視 ② 内部から外部への接続監視 (4) 認証デバイス紛失時の対応 接続先の本人確認に使用する認証デバイス(MFAデバイス等)を本人が紛失した際の対応策を定める。 (5) 脆弱性等への対応 外部と接続するサーバやルータ等に搭載されているソフトウェアについて、脆弱性等の情報を収集し、適切なバージョンアップを行うなどの対応策を定める。Amazon Linuxを利用の場合、AWSではAmazon Linux Security Center(※2)にて脆弱性情報を入手してください。また、外部からの不正アクセス等により生じた損害賠償責任、逸失利益、業務継続に要した費用等について、保険の加入を検討することが望ましい。 [参考文献、参考URL] (※1)AWS Trusted Advisor https://aws.amazon.com/jp/premiumsupport/technology/trusted-advisor/ (※2)Linux Security Center https://alas.aws.amazon.com/
実35	○	○	AWSではAWS 人事管理システムのオンボーディングワークフロープロセスの一環として、一意のユーザー ID が作成されます。デバイスプロビジョニングプロセスは、デバイスの ID を確実に一意にするうえで役立ちます。両方のプロセスとも、ユーザーアカウントまたはデバイスを確立するためのマネージャーの承認が含まれます。最初の認証は、プロビジョニングプロセスの一部としてユーザーに対面で提供されるとともに、デバイスにも提供されます。内部ユーザーは SSH パブリックキーをアカウントに関連付けることができます。システムカウントの認証は、リクエスタの ID を確認した後で、アカウント作成プロセスの一部としてリクエスタに提供されます。 物理的アクセスは、建物の周辺および入り口において、監視カメラや侵入検知システムなどの電子的手段を用いる専門の保安要員その他の手段により、厳重に管理されています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。 AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO/IEC 27001、およびFedRAMPsm への準拠のため、監査中に外部の独立監査人によって確認されます	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実36	○	○	AWS は、変更の管理にシステム的なアプローチを採用しています。そのためお客様に影響を与えるサービスの変更は、徹底的に検証、テスト、承認され、充分な情報が提供されます。変更の実稼動環境への投入は通常、最も影響の小さいエリアへの段階的配備から開始されます。デプロイは単一のシステムでテストされ、影響が評価できるよう綿密にモニタリングされます。 AWS変更管理アプローチでは、変更が本番環境にデプロイされる前に、次の手順を完了する必要があります。 1.適切なAWS変更管理ツールを通じて変更を文書化し、伝達します。 2.混乱を最小限に抑えるために、変更およびロールバック手順の実装を計画します。 3.論理的に分離された非運用環境で変更をテストします。 4.ビジネスへの影響と厳密な技術に重点を置いて、変更のピアレビューを完了します。レビューにはコードレビューを含める必要があります。 5.権限のある者による変更の承認を得 ます。 社員が個々の役割と責任を理解するのを助けるため、ISO/IEC 27001に準拠した、完了確認を必要とする定期的な情報セキュリティトレーニングを実施しています。従業員が確立された ポリシーを理解し、従っているかについてはコンプライアンス監査が定期的に行われます。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実37	○	○	AWS は、変更の管理にシステム的なアプローチを採用しています。そのためお客様に影響を与えるサービスの変更は、徹底的に検証、テスト、承認され、充分な情報が提供されます。変更の実稼動環境への投入は通常、最も影響の小さいエリアへの段階的配備から開始されます。デプロイは単一のシステムでテストされ、影響が評価できるよう綿密にモニタリングされます。 可能な場合、変更は通常の変更時間帯に予定されます。標準の変更管理手順と異なる手順を必要とする実稼動システムに対する緊急の変更は、インシデントと関連付けられており、必要に応じて記録され、承認されます。 AWS は、重要なサービスの変更に対する自己監査を定期的に行っており、品質をモニタリングしながら高い基準を維持することによって、変更管理プロセスの継続的な改善に貢献しています。例外は分析され、根本的な原因が決定さ れて適切な措置が取られます。変更はコンプライアンスに従うようにされるか、または必要に応じてロールバックされます。その後プロセスまたは人的問題を解決して修正するための措置が取られます。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実38	○	○	すべてのアクティビティはセキュリティレビューのために記録されます。また、AWS 従業員によるデータセンターへのすべての物理的アクセスは記録され、定期的に監査されます	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	[概要] オンプレミスと同様に、依頼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須です。 [対策例] ■オペレーションの記録 ・AWS CloudTrailを用いてAWSの操作状況を自動的にログ出力します。 ・Amazon EC2インスタンスを利用する場合は、AWS Systems Manager Session Managerを利用してSSHなどでの操作状況をログ出力します。 ・構成管理において、AWS Configを利用して設定変更のログを出力します。 ・運用PCにおいて、AWS Management Consoleの画面キャプチャを記録します。 ■オペレーションの記録の確認 ・Amazon S3内のログに対して、Amazon Athenaを利用して標準のSQLを使用して記録内容を確認することができます。 ・CloudWatch Logs内のログに対して、CloudWatch Logs Insightsを利用して記録内容を確認することができます。 ・オペレーションに関する不正検知としてAmazon GuardDutyを利用し、セキュリティ状況の把握にAWS Security Hubを利用することができます。 ■AWSのオペレーションの状況確認 ・AWS自身のオペレーションにおけるセキュリティ対応やコンプライアンスの遵守状況については、利用者側が確認するものとして、AWS Artifactを利用することができます。 [参考文献、参照URL] ・AWS CloudTrail ユーザーガイド https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/best-practices-security.html ・AWS Systems Manager Session Manager ユーザーガイド https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/session-manager.html ・Athena を使用して Amazon S3 サーバーのアクセスログを分析するにはどうすればよいですか? https://aws.amazon.com/jp/premiumsupport/knowledge-center/analyze-logs-athena/ ・Amazon CloudWatch Logsユーザーガイド https://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html ・CloudWatch Logs Insights を使用したログデータの分析 https://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/logs/AnalyzingLogData.html ・Amazon GuardDuty https://aws.amazon.com/jp/guardduty/ ・AWS Security Hub https://aws.amazon.com/jp/security-hub/ ・AWS Artifact https://aws.amazon.com/jp/artifact/
実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 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の「11.責任限定」において、データの損失に関して記載されています。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。 [関連する認証] ・ISO 27001 -12.3 バックアップ [参考文献、参照URL] ・金融機関向け AWS FISC安全対策基準対応リファレンス https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_FISC_Guidelines_9thEdition.pdf ・AWS カスタマーアグリーメント https://d1.awsstatic.com/legal/aws-customer-agreement/AWS_Customer_Agreement_Japanese_Translation2.pdf	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報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] データファイル障害及び災害等への対応のため、コンティンジェンシープランと整合性のとれた適切な保管期間、保管サイクル、保管場所でバックアップを取得し、管理方法を明確にします。 [対策例] AWSに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、リージョンを跨いでのバックアップを検討する。なお、日本国外とのクロスリージョンにおいては、個人情報等の機微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ります。 ・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ログを取得する。 なお、バックアップデータの保管場所においては、セキュリティ・対障害性・可用性(保管データの取り出しに掛かる時間)、コストについて考慮する必要があります。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。 [参考文献、参照URL] ・AWS Backup https://docs.aws.amazon.com/ja_jp/aws-backup/latest/devguide/whatisbackup.html ・Amazon Data Lifecycle Manager https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/snapshot-lifecycle.html ・個人情報の保護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編) 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=sn&loc=3
実40	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実41	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実42	○	○	AWS は、変更の管理にシステム的なアプローチを採用しています。そのためお客様に影響を与えるサービスの変更は、徹底的に検証、テスト、承認され、充分な情報が提供されます。AWS の変更管理プロセスは、意図しないサービス障害を防ぎ、お客様に対するサービスの完全性を維持することを目的としています。AWS は、重要なサービスの変更に対する自己監査を定期的に行っており、品質をモニタリングしながら高い基準を維持することによって、変更管理プロセスの継続的な改善に資献しています。例外は分析され、根本的な原因が決定されて適切な措置が取られます。変更はコンプライアンスに従うようにされるか、または必要に応じてロールバックされます。その後プロセスまたは人的問題を解決して修正するための措置が取られます。	[概要] AWSは、AWSの責任範囲において、ネットワーク機器を管理します。金融機関等は、AWSの責任範囲に含まれるネットワーク機器のAWSの側の管理方法について、以下の観点から確認が必要です。 ・変更管理(変更手続き、設定変更手順、バックアップ計画等) ・稼働監視 ・機器(ルータ等)へのアクセス管理 このうち、AWSの対応において言及されていない機器(ルータ等)へのアクセス管理に関する対応状況については、SOC2レポート等から把握することができます。 [参考文献、URL] ・AWS Well-Architected フレームワーク セキュリティの柱 https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/wellarchitected-security-pillar.pdf ・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/wellarchitected-reliability-pillar.pdf ※AWS Well-Architected は、クラウドアーキテクトがアプリケーションやワークロード向けに高い安全性、性能、障害耐性、効率性を備えたインフラストラクチャを構築する際に役立ちます。AWS Well-Architected では、5 つの柱(優れた運用効率、セキュリティ、信頼性、パフォーマンス効率、コストの最適化)に基づいて、お客様とパートナーがアーキテクチャを評価し、時間と共に拡大できる設計を実装するための一貫したアプローチを提供しています。	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 お客様はAWSリソースの管理にAWS Configを使用することができます。AWS Configは、セキュリティとガバナンスのためのフルマネージド型のサービスであり、ご利用のAWS リソースのインベントリ、構成履歴、構成変更通知の機能を備えています。AWS Config では、既存の AWS リソースの特定や、構成の詳細すべてを含めたお客様の AWS リソースインベントリのエクスポートが可能になり、特定の時点でどのようにリソースが構成されたかを判断できます。これらの機能は、コンプライアンス監査、セキュリティ分析、リソース変更の追跡、トラブルシューティングを可能にします。	[概要] ネットワークの設定情報の管理を行う必要があります。 ネットワーク設定情報の不正な変更への対応のため、設定情報を適切に管理する必要があります。 クラウド内のネットワークやAWSサービス等の変更や保守作業時の人的ミスやサイバー攻撃によりネットワーク設定情報が不正な状態に設定され、セキュリティリスクが高まる懸念があります。 クラウドサービスでは各サービスで提供されているサービスを利用して、システムの構成や設定変更を監視を行いポリシーに従った監査・修正することができるようになっており、これらサービスへの安全なアクセス方法を明確にする必要があります。 ■AWSサービスを利用した対応 ●AWS Configサービスの概要 （※1） ●AWS Security Hubサービスの概要 （※2） ●AWS Trusted Advisorサービスの概要 （※3） ■他サービスを利用した対応 ●Cloud Security Posture Management(CSPM)ソリューションの導入 [参考文献、参照URL] (※1)https://aws.amazon.com/jp/config/features/ (※2)https://aws.amazon.com/jp/security-hub/features/
実43	○	○	内部的には、AWSネットワークセグメンテーションはISO/IEC 27001に準拠しています。詳細については、ISO/IEC 27001の附属書A.ドメイン13を参照してください。 AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 AWS は、変更の管理にシステム的なアプローチを採用しています。そのためお客様に影響を与えるサービスの変更は、徹底的に検証、テスト、承認され、充分な情報が提供されます。AWS の変更管理プロセスは、意図しないサービス障害を防ぎ、お客様に対するサービスの完全性を維持することを目的としています。実稼働環境にデプロイされる変更には、以下の対応が行われます: - 検証: 変更の技術的側面について専門家による検証が必要です。 - テスト: 適用されている変更は、予想どおりに動作し、パフォーマンスに悪影響を与えないことを確認するためにテストされます。 - 承認: すべての変更は、ビジネスへの影響を適切に監視し、それらの影響についての情報を提供するために、承認される必要があります。	[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の「11.責任限定」において、データの損失に関して記載されています。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。 [関連する認証] ・ISO 27001 -12.3 バックアップ [参考文献、参照URL] ・金融機関向け AWS FISC安全対策基準対応リファレンス https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_FISC_Guidelines_9thEdition.pdf ・AWS カスタマーアグリーメント https://d1.awsstatic.com/legal/aws-customer-agreement/AWS_Customer_Agreement_Japanese_Translation2.pdf	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 お客様はAWSリソースの管理にAWS Configを使用することができます。AWS Configは、セキュリティとガバナンスのためのフルマネージド型のサービスであり、ご利用のAWS リソースのインベントリ、構成履歴、構成変更通知の機能を備えています。AWS Config では、既存の AWS リソースの特定や、構成の詳細すべてを含めたお客様の AWS リソースインベントリのエクスポートが可能になり、特定の時点でどのようにリソースが構成されたかを判断できます。これらの機能は、コンプライアンス監査、セキュリティ分析、リソース変更の追跡、トラブルシューティングを可能にします。	[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の利用が有効です。 リージョン障害などの大規模障害を想定した場合は、設計資料と、パラメータの遠隔保管も合わせて実施します。 設定情報を含むファイルのバックアップについては実39記載内容を参照下さい。 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ーの運用、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 [対策例] 1) AWS Configの構成管理機能の利用 2) ネットワーク構成図、設計・設定パラメータシートの保管 3) AWS CLIにより設定情報を取得、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44	○	○	AWS は、AWS 製品の設計、開発、運用において、優れた商用 IT プラクティスを確実に活用する責任があります。 AWS は、お客様の信頼と信頼の維持を最も重要視しているため、可用性、完全性、機密性の観点から AWS 製品の品質属性を定義します。 AWS 品質システムは、組織構造、責任、手順、プロセス、リソースなど、AWS が品質管理を実装するために必要な要素に対応します。 AWS は、国際標準化機構（ISO）によって確立されたベストプラクティスガイドラインを満たす、またはそれ以上の品質管理システムを確立しています。 品質管理システムは、AWS サービス、AWS インフラストラクチャ、AWS サービスの開発と運用をサポートするアセットを含む AWS 製品の開発と運用に適用されます。 品質マネジメントシステムに適用される主要な規格には、ISO 9001、ISO/IEC 27001、ISO/IEC 27017、ISO/IEC 27018 があります。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実45	○	○	AWS のインシデント対応プログラム、計画、および手続きは、ISO/IEC 27001 に準拠しています。AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 詳細については、”アマゾン ウェブ サービス :セキュリティプロセスの概要 “ホワイトペーパー(http://aws.amazon.com/security で入手可能) を参照してください。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実46	○	○	AWS モニタリングツールは、異常な、または不正なアクティビティと条件を通信の出入り口で検出するように設計されています。これらのツールは、サーバーおよびネットワークの利用状況、ポートスキャニングアクティビティ、アプリケーションの利用状況、および許可されていない侵入の試みをモニタリングします。このツールを使用して、異常なアクティビティに対して独自に性能測定基準のしきい値を設定することができます。 AWS 内のシステムには膨大な装置が備わっており、主要なオペレーションメトリックをモニタリングしています。主要なオペレーションメトリックが早期警告しきい値を超えた場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。オンコールスケジュール（常時待機体制）が採用されているので、担当者が運用上の問題にいつでも対応することができます。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 AWS Cloudwatchは、AWSのクラウド資源及びお客様が運用するアプリケーションに対するモニタリングを提供しま す。また、AWSはサービス提供の最新の状況をAWS Service Health Dashboard(https://status.aws.amazon.com/)にて公開しています。	[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ような監視体制の整備が可能です。 [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。 ■システムの脅威検知 ・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な可視化 ・AWS Security Hubを利用し、AWS環境のセキュリティ対応上場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。

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
						[参考文献、参照URL] ・Amazon CloudWatch ユーザーガイド https://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html ・Amazon GuardDuty https://aws.amazon.com/jp/guardduty/ ・AWS Security Hub https://aws.amazon.com/jp/security-hub/ ・Amazon Detective https://aws.amazon.com/jp/detective/
実47	○	○	AWS モニタリングツールは、異常な、または不正なアクティビティと条件を通信の出入り口で検出するように設計されています。これらのツールは、サーバーおよびネットワークの利用状況、ポートスキャニングアクティビティ、アプリケーションの利用状況、および許可されていない侵入の試みをモニタリングします。このツールを使用して、異常なアクティビティに対して独自に性能測定基準のしきい値を設定することができます。 AWS 内のシステムには膨大な装置が備わっており、主要なオペレーションメトリックをモニタリングしています。主要なオペレーションメトリックが早期警告しきい値を超えた場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。オンコールスケジュール（常時待機体制）が採用されているので、担当者が運用上の問題にいつでも対応することができます。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 AWS Cloudwatchは、AWSのクラウド資源及びお客様が運用するアプリケーションに対するモニタリングを提供しま す。 また、AWSはサービス提供の最新の状況をAWS Service Health Dashboard(https://status.aws.amazon.com/)にて公開しています。	[概要] 各種資源の使用状況、健全性を監視します。 [対策例] ・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。 ・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、サードパーティー製ツール等の導入も検討します。 ・AWS全体のサービス稼働状況はService Health Dashboardで確認しつつ、利用するアカウントごとに影響を確認する場合はAWS Personal Health Dashboardも利用します。 ・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。 [参考文献、参考URL] ・AWS Service Health Dashboard https://status.aws.amazon.com/ ・AWS Personal Health Dashboard の使用 https://docs.aws.amazon.com/ja_jp/health/latest/ug/getting-started-phd.html
実48	○	○	AWSはISO/IEC 27001 に準拠して、AWS の担当者が AWS 専有インベントリ管理ツールを使用して、AWS ハードウェアの資産に所有者を割り当て、追跡および監視を行っています。AWS の調達およびサプライチェーンチームは、すべての AWS サプライヤとの関係を維持しています。 追加の詳細については、ISO/IEC 27001の附属書 A. 8を参照してください。AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 AWS Systems Manager を使用することで、複数の AWS のサービスの運用データを一元化し、AWS リソース全体のタスクを自動化できます。アプリケーション、アプリケーションスタックのさまざまなレイヤー、本番環境と開発環境といったリソースの論理グループを作成できます。Systems Manager では、リソースグループを選択し、その最新の API アクティビティ、リソース設定の変更、関連する通知、運用アラート、ソフトウェアインベントリ、パッチコンプライアンス状況を表示できます。運用ニーズに応じて、各リソースグループに対してアクションを実行することもできます。Systems Manager により、AWS リソースを一元的に表示および管理でき、運用を完全に可視化して制御できます。	[概要] ・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。 [対策例] ■AWSサービスの構成管理 ・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、有効期限が存在するサービスについては、有効期限の確認を行うことが必要です。 ・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。 ・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るサービスがあります。 ■テナント側の構成管理 ・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。 ・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。
実49	○	-	・AWSはISO/IEC 27001 に準拠して、AWS の担当者が AWS 専有インベントリ管理ツールを使用して、AWS ハードウェアの資産に所有者を割り当て、追跡および監視を行っています。AWS の調達およびサプライチェーンチームは、すべての AWS サプライヤとの関係を維持しています。 追加の詳細については、ISO/IEC 27001の附属書 A. 8を参照してください。AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 ・AWS のデータセンターは、外部からはそれとはわからないようになっています。ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。 ・AWS は、権限を持つ担当者のみにデータセンターへの物理的なアクセスを許可しています。データセンターへのアクセスを必要とするすべての担当者は、まずアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最少権限の原則に基づき許可されますが、個人がアクセスを必要とするデータセンターのレイヤーを指定する必要があり、アクセスの期限が設定されます。申請は権限を持つ人物のみが審査して承認し、請求した期限が過ぎた後は、アクセスが取り消されます。入場を許可された担当者は、その権限で指定されたエリアのみに入場が制限されます。	[関連する認証] ・ISO/IEC 27001 -8 資産の管理 -11.2 装置	-	-
実50	○	-	・AWSはISO/IEC 27001 に準拠して、AWS の担当者が AWS 専有インベントリ管理ツールを使用して、AWS ハードウェアの資産に所有者を割り当て、追跡および監視を行っています。AWS の調達およびサプライチェーンチームは、すべての AWS サプライヤとの関係を維持しています。 追加の詳細については、ISO/IEC 27001の附属書 A. 8を参照してください。AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 ・AWS のデータセンターは、外部からはそれとはわからないようになっています。ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。 ・AWS は、権限を持つ担当者のみにデータセンターへの物理的なアクセスを許可しています。データセンターへのアクセスを必要とするすべての担当者は、まずアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最少権限の原則に基づき許可されますが、個人がアクセスを必要とするデータセンターのレイヤーを指定する必要があり、アクセスの期限が設定されます。申請は権限を持つ人物のみが審査して承認し、請求した期限が過ぎた後は、アクセスが取り消されます。入場を許可された担当者は、その権限で指定されたエリアのみに入場が制限されます。	[関連する認証] ・ISO/IEC 27001 -8 資産の管理 -11.2 装置	-	-

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実51	○	-	・AWS は電気および機械に関連する設備をモニタリングし、予防的なメンテナンスを実施して、AWS データセンター内のシステムの継続的な運用性を維持しています。機器のメンテナンス手順は資格を持っている担当者が実行し、文書化されたメンテナンススケジュールに従って完了されます。 ・AWS では、定期的な保守やシステムのパッチ適用を実行するために、システムをオフラインにする必要がありません。通常、AWS の保守およびシステムのパッチ適用はお客様に影響がありません。 インスタンスの保守自体は、お客様が統制します。 ・In order to ensure maintenance procedures are properly executed, AWS assets are assigned an owner, tracked and monitored with AWS proprietary inventory management tools. AWS asset owner procedures are carried out by method of utilizing a proprietary tool with specified checks that must be completed according to the documented maintenance schedule. Third party auditors test AWS equipment maintenance controls by validating that the asset owner is documented and that the condition of the assets are visually inspected according to the documented maintenance policy. （参考訳）保守作業が適切に実施されていることを検証するために、AWS専用インベントリ管理ツールを使用して、AWSのアセットに所有者を割り当て、追跡および監視を行っています。文書化された保守スケジュールに沿って検証が実施できるように、専用ツールを使ってAWSアセット所有者の作業を管理しています。独立した監査人はAWSの機器の保守に対する統制を検証しています。この検証ではアセットに所有者が割り当てられ、文書化された保守作業のポリシーに従ってアセットの状態が目視で検証されていることをチェックします。	[関連する認証] ・ISO/IEC 27001 -8 資産の管理 -11.2 装置	-	-
実52	○	-	AWS は電気および機械に関連する設備をモニタリングし、予防的なメンテナンスを実施して、AWS データセンター内のシステムの継続的な運用性を維持しています。機器のメンテナンス手順は資格を持っている担当者が実行し、文書化されたメンテナンススケジュールに従って完了されます。	[関連する認証] ・ISO/IEC 27001 -8 資産の管理 -11.2 装置	-	-
実53	○	-	・AWSはISO/IEC 27001 に準拠して、AWS の担当者が AWS 専有インベントリ管理ツールを使用して、AWS ハードウェアの資産に所有者を割り当て、追跡および監視を行っています。AWS の調達およびサプライチェーンチームは、すべての AWS サプライヤとの関係を維持しています。追加の詳細については、ISO/IEC 27001の附属書 A. 8を参照してください。AWS は ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 ・データセンターに対する物理的なアクセスを権限のある人物のみ制限し、故障や物理的な災害がデータセンター施設に与える影響を最小限に抑えるメカニズムが存在するように統制によって適切な保証を実現します。 ・AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。 ・データセンターの電力システムは、完全に冗長性をもち、運用に影響を与えることなく管理が可能となっています。1日24時間体制で、年中無休で稼働しています。施設内で重要かつ不可欠な負荷に対応するために、電力障害時には無停電電源装置（UPS）がバックアップ電力を供給しています。データセンターは、発電機を使用して施設全体のバックアップ電力を供給しています。 ・サーバーその他のハードウェアの運用温度を一定に保つために、空調制御が必要です。これによって過熱を防ぎ、サーバー停止の可能性を減らすことができます。データセンターは、大気の状態を最適なレベルに保つように設定されています。作業員とシステムが、温度と湿度を適切なレベルになるように監視してコントロールしています。	[関連する認証] ・ISO/IEC 27001 -8 資産の管理 -11.2 装置 [参考文献、参照URL] ・AWSのコントロール https://aws.amazon.com/jp/compliance/data-center/controls/	-	-
実54	○	-	AWS は、AWS インフラストラクチャ、データセンター、およびサービスを対象とした Information Security Management System (ISMS) の ISO/IEC 27001 認証を取得しています。 AWS は電気および機械に関連する設備をモニタリングし、予防的なメンテナンスを実施して、AWS データセンター内のシステムの継続的な運用性を維持しています。機器のメンテナンス手順は資格を持っている担当者が実行し、文書化されたメンテナンススケジュールに従って完了されます。 また、問題の速やかな特定を可能にするため、電気的、機械的なシステムおよび設備をモニタリングしています。これは継続的な監査ツールと、建物管理および電気的なモニタリングシステムを通じて提供される情報を利用して行われます。予防的メンテナンスが実行され、設備の運用に関しての継続性が保たれています。 データセンター環境の物理的な管理方法については、SOC1 Type2 reportの以下にも記載しております。 E. Physical Security and Environmental Protection ・Environment Management	-	-	-
実55	○	-	AWS は、AWS インフラストラクチャ、データセンター、およびサービスを対象とした Information Security Management System (ISMS) の ISO/IEC 27001 認証を取得しています。 Amazonのデータセンターは最新式で、革新的で建築的かつ工学的アプローチを採用しています。Amazon は大規模データセンターの設計、構築、運用において、長年の経験を有しています。この経験は、AWS プラットフォームとインフラストラクチャに活かされています。データセンター設備は問題が速やかに特定されるように、電気、機械、ライフサポートシステムおよび設備を監視しています。予防的メンテナンスが実行され、設備を継続的な運用性が保たれています。 火災検出と鎮火 自動火災検出および鎮火装置が取り付けられ、リスクを軽減しています。この火災検出システムは、全データセンター環境、機械的及び電気的インフラストラクチャースペース、冷却室および発電機設備室において、煙検出センサーを使用しています。これらのエリアは、充水型、二重連結予作動式、またはガス式スプリンクラーシステムによって守られています。 電力 データセンターの電力システムは、完全に冗長性をもち、運用に影響を与えることなく管理が可能となっています。1日24時間体制で、年中無休で稼動しています。施設内で重要かつ不可欠な負荷に対応するために、電力障害時には無停電電源装置（UPS）がバックアップ電力を供給しています。データセンターは、発電機を使用して施設全体のバックアップ電力を供給しています。 空調と温度 サーバーその他のハードウェアの運用温度を一定に保つために、空調制御が必要です。これによって過熱を防ぎ、サーバー停止の可能性を減らすことができます。データセンターは、大気の状態を最適なレベルに保つように設定されています。作業員とシステムが、温度と湿度を適切なレベルになるよう監視してコントロールしています。 物理的な環境保護の統制に対する監査レポートとして、SOC1 Type2 reportの以下にも記載しております。 ・Control Objective 5: Physical Security and Environmental Protection No7~No12	[関連する認証] ・ISO/IEC 27001 -8 資産の管理 -11.2 装置 [参考文献、参照URL] ・AWSのコントロール https://aws.amazon.com/jp/compliance/data-center/controls/	-	-

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実56	○	-	AWS は、AWS インフラストラクチャ、データセンター、およびサービスを対象とした Information Security Management System (ISMS) の ISO/IEC 27001 認証を取得しています AWSのデータセンターでは、ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。 AWS は、権限を持つ担当者のみにデータセンターへの物理的なアクセスを許可しています。データセンターへのアクセスを必要とするすべての担当者は、まずアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最少権限の原則に基づき許可されますが、個人がアクセスを必要とするデータセンターのレイヤーを指定する必要があり、アクセスの期限が設定されます。申請は権限を持つ人物のみが審査して承認し、請求した期限が過ぎた後は、アクセスが取り消されます。入場を許可された担当者は、その権限で指定されたエリアのみに入場が制限されます。	-	-	-
実57	○	-	AWS は、AWS インフラストラクチャ、データセンター、およびサービスを対象とした Information Security Management System (ISMS) の ISO/IEC 27001 認証を取得しています AWSのデータセンターでは、ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。 AWS は、権限を持つ担当者のみにデータセンターへの物理的なアクセスを許可しています。データセンターへのアクセスを必要とするすべての担当者は、まずアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最少権限の原則に基づき許可されますが、個人がアクセスを必要とするデータセンターのレイヤーを指定する必要があり、アクセスの期限が設定されます。申請は権限を持つ人物のみが審査して承認し、請求した期限が過ぎた後は、アクセスが取り消されます。入場を許可された担当者は、その権限で指定されたエリアのみに入場が制限されます。 第三者のアクセスについては、承認された AWS の担当者が申請する必要があり、その担当者は第三者によるアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最少権限の原則に基づいて付与されます。申請では個人がアクセスを必要とするデータセンターのレイヤーを指定する必要があり、期限が設定されます。これらの申請は権限を持つ人物のみが審査して承認し、請求した期限が過ぎた後は、アクセスが取り消されます。入場を許可された担当者は、その権限で指定されたエリアのみ入場できます。訪問者バッジを与えられた担当者は、現場への到着後身分証明書を提示します。署名後に入場が許可され、権限を持つスタッフが常に付き添います。	-	-	-
実58	○	-	AWS は、AWS インフラストラクチャ、データセンター、およびサービスを対象とした Information Security Management System (ISMS) の ISO/IEC 27001 認証を取得しています AWSのデータセンターでは、ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。 AWS は、権限を持つ担当者のみにデータセンターへの物理的なアクセスを許可しています。データセンターへのアクセスを必要とするすべての担当者は、まずアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最少権限の原則に基づき許可されますが、個人がアクセスを必要とするデータセンターのレイヤーを指定する必要があり、アクセスの期限が設定されます。申請は権限を持つ人物のみが審査して承認し、請求した期限が過ぎた後は、アクセスが取り消されます。入場を許可された担当者は、その権限で指定されたエリアのみに入場が制限されます。 第三者のアクセスについては、承認された AWS の担当者が申請する必要があり、その担当者は第三者によるアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最少権限の原則に基づいて付与されます。申請では個人がアクセスを必要とするデータセンターのレイヤーを指定する必要があり、期限が設定されます。これらの申請は権限を持つ人物のみが審査して承認し、請求した期限が過ぎた後は、アクセスが取り消されます。入場を許可された担当者は、その権限で指定されたエリアのみ入場できます。訪問者バッジを与えられた担当者は、現場への到着後身分証明書を提示します。署名後に入場が許可され、権限を持つスタッフが常に付き添います。	-	-	-
実59	○	-	セキュリティを保つべき領域での作業に関する管理策はISO/IEC 27001に規定されており、AWSのデータセンターにおける運用管理策についてはISO/IEC 27001認証を取得しています。詳細については ISO/IEC 27001 の附属書 A.11.1.5 をご参照ください。 すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。AWSは、そのような権限に対して正規のビジネスニーズがある従業員や業者に対してのみデータセンターへのアクセスや情報を提供しています。従業員がこれらの特権を必要とする作業を完了すると、その後に Amazon またはアマゾン ウェブ サービスの従業員となり続ける場合であっても、そのアクセス権は速やかに取り消されます。 AWS データセンターへの物理アクセスは、記録、監視され、そうした情報は保持されることになります。AWS は論理的および物理的なモニタリングシステムから取得した情報を、必要に応じてセキュリティを向上させるために相関性を確認します。 AWS ではグローバルセキュリティオペレーションセンターを使用してデータセンターを監視しています。このグローバル・セキュリティ・オペレーションセンターは、モニタリング、対処優先順位の決定、および決定された処理を実施について責任をもっています。データセンターのアクセスを管理、モニタリングし、ローカルのチームと関連サポートチームと協力し、対処優先順位の決定、コンサルティング、分析、送信を行い、24 時間 365 日グローバルレベルのサポートを提供しています。	-	-	-

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実60	○	-	・火災検出と鎮火 自動火災検出および鎮火装置が取り付けられ、リスクを軽減しています。この火災検出システムは、全データセンター環境、機械的及び電気的インフラストラクチャースペース、冷却室および発電機設備室において、煙検出センサーを使用しています。これらのエリアは、充水型、二重連結予作動式、またはガス式スプリンクラーシステムによって守られています。 ・電力 データセンターの電力システムは、完全に冗長性をもち、運用に影響を与えることなく管理が可能となっています。1日24 時間体制で、年中無休で稼動しています。施設内で重要かつ不可欠な負荷に対応するために、電力障害時には無停電電源装置（UPS）がバックアップ電力を供給しています。データセンターは、発電機を使用して施設全体のバックアップ電力を供給しています。 ・空調と温度 サーバーその他のハードウェアの運用温度を一定に保つために、空調制御が必要です。これによって過熱を防ぎ、サーバー停止の可能性を減らすことができます。データセンターは、大気の状態を最適なレベルに保つように設定されています。作業員とシステムが、温度と湿度を適切なレベルになるよう監視してコントロールしています。 ・管理 AWS は、問題が速やかに特定されるように、電気、機械、ライフサポートシステムおよび設備を監視しています。予防的メンテナンスが実行され、設備の継続的な運用性が保たれています。	[概要] AWSはデータセンターの各種設備に対する監視体制を構築しており、ISO/IEC 27001を含む各種認証を取得しています。 FISC安全対策基準で示されている各監視対象について、その準拠性を具体的に示した情報は公開されていませんが、データセンターにおける物理的、環境的コントロールはAWSのwebサイト、ホワイトペーパー、SOC2レポート等から把握することができます。 [関連する認証] ・ISO/IEC 27001 -8 資産の管理 -11.2 装置 [参考文献、参照URL] ・AWSのコントロール https://aws.amazon.com/jp/compliance/data-center/controls/	-	-
実61	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実62	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実63	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実64	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実65	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実66	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実67	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実68	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実69	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実70	○	○	AWS は、様々な手段の外部コミュニケーションを実施して、その顧客ベースとコミュニティをサポートしてきました。カスタマーエクスペリエンスに影響を与える運用上の問題についてカスタマーサポートチームが通知受けることができるようにするためのメカニズムが配備されています。[Service Health Dashboard] が、顧客サポートチームによって管理運営されており、大きな影響を与える可能性のある問題について顧客に警告を発することができます。 カスタマーサポートチームと直接連絡を取ったり、お客様に影響を与える各種の問題に対する警告を事前に受け取ることができる AWS サポートに申し込みをすることもできます。 AWSは、様々な方法でグローバルレベルの内部コミュニケーションを実施することで、従業員が各自の役割と責任を理解することを手助けし、重要なイベントについて適時伝達しています。	[概要] AWSは障害時、災害時における連絡体制を構築しており、ISO/IEC 27001を含む各種認証を取得しています。また、関係者への連絡を含むインシデント発生時の対応については、SOC2レポート等から把握することができます。 [関連する認証] ・ISO/IEC 27001 -6.1 資産の管理 -16.1 装置	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 AWS サポートは、経験豊富な技術サポートエンジニアによる、1 対 1 の迅速なレスポンスを特徴とするサポートサービスです。AWS サポートは、お客様がそのインフラストラクチャをクラウドで運用できるように技術的な問題に関する支援を行います。操作上の問題や技術的な質問があるお客様は、サポートエンジニアのチームに連絡でき、予測可能な応答時間およびパーソナライズされたサポートを受けることができます。 AWSサポートの詳細については以下のURLをご参照ください。（ https://aws.amazon.com/jp/premiumsupport/ ）	-
実71	○	○	事業継続マネジメントに関する管理策はISO/IEC 27001に準拠しており、AWSのデータセンターにおける運用管理策については ISO/IEC 27001認証を取得しています。ISO/IEC 27001の内容については ISO/IEC 27001 の附属書 A.17 をご参照ください。 Amazon のインフラストラクチャは高いレベルの可用性を備え、回復機能を持つ IT アーキテクチャを配備する機能を顧客に提供します。AWS のシステムは、お客様への影響を最小限に抑えながらシステムまたはハードウェア障害に耐えられるように設計されています。また、AWS におけるデータセンターの事業の継続性は、Amazon Infrastructure Group の指示に従って管理されます。 世界各地に設置されているデータセンターは、所在地によりリージョンに分けられています。すべてのデータセンターは オンラインでお客様にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動されます。重要なアプリケーションは N+1 原則でデプロイさ れます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。 AWS を使用すると、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理上のリージョン内に、柔軟にインスタンスを配置してデータを保管できます。各アベイラビリティーゾーンは、障害が発生しても他のゾーンに影響を与えないように設計されています。つまり、アベイラビリティゾーンは、代表的な都市のリージョン内で物理的に区切られており、低リスクの氾濫原にあります(具体的な洪水帯の分類はリージョンによって異なります)。個別の無停電電源装置(UPS)やオンサイトのバックアップ生成施設に加え、シングルポイントの障害の可能性を減らすために、別々の電力供給施設から異なる配管網を経由して、個別に電力供給を行っています。アベイラビリティゾーンはすべて、複数の Tier-1 トランジットプロバイダに重複して接続しています。 AWS のバックアップおよび冗長性メカニズムは、ISO/IEC 27001 に準拠して開発され、テストされています。AWS のバックアップおよび冗長性メカニズムに関する追 加情報については、ISO/IEC 27001 の付録 A、ドメイン 12 および AWS SOC 2 レ ポートを参照してください。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 AWS サポートは、経験豊富な技術サポートエンジニアによる、1 対 1 の迅速なレスポンスを特徴とするサポートサービスです。AWS サポートは、お客様がそのインフラストラクチャをクラウドで運用できるように技術的な問題に関する支援を行います。操作上の問題や技術的な質問があるお客様は、サポートエンジニアのチームに連絡でき、予測可能な応答時間およびパーソナライズされたサポートを受けることができます。 AWSサポートの詳細については以下のURLをご参照ください。（ https://aws.amazon.com/jp/premiumsupport/ ）	[概要] 金融機関にて、BCP/DRに関連して以下の対策例を検討する必要があります。 [対策例] ■AWSでのBCP/DRで取り得る施策の確認と災害対策の方式設計 ・AWSではBCP/DRの施策として、マルチリージョンやマルチAZ等のファシリティと、 AWS Backup等のバックアップ/リカバリやデータ同期の様々のマネージドサービスを用意しています。 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への切替マニュアル整備 ■インシデントの一次切り分けや復帰時の責任分担の整備 ・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(最重要は金融庁に報告)など ■定期的に切替訓練の実施や、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=ngi&loc=2

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実72	○	○	AWSのインシデント管理チームは、業界標準の診断手順を採用しており、事業に影響を与えるイベント時に解決へと導きます。作業員スタッフが、24 時間 365 日体制でインシデントを検出し、影響と解決方法を管理します。 インシデントや問題の処理時には、運用担当者を支援して情報を提供するための文書が保持されます。問題の解決のために協力体制が必要な場合は、情報伝達と記録機能をサポートする会議システムが使用されます。協力体制を必要とする運用上の問題の処理にあたっては、訓練を受けた通話リーダーが、コミュニケーションと進捗を支援します。 深刻な運用上の問題が発生した後には、外部的な影響の有無に関わらず、事後分析会議が開かれます。そして エラーの原因（COE）に関する文書が起草され、根本的な原因が捕捉されて、今後のために予防措置が取られるようにします。予防措置の実施は、週に一度開かれる運用会議において追跡されます。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 AWS サポートは、経験豊富な技術サポートエンジニアによる、1 対 1 の迅速なレスポンスを特徴とするサポートサービスです。AWS サポートは、お客様がそのインフラストラクチャをクラウドで運用できるように技術的な問題に関する支援を行います。操作上の問題や技術的な質問があるお客様は、サポートエンジニアのチームに連絡でき、予測可能な応答時間およびパーソナライズされたサポートを受けることができます。 AWSサポートの詳細については以下のURLをご参照ください。 （ https://aws.amazon.com/jp/premiumsupport/ ）	[概要] 稼働状況を確認し、障害の発生原因の記録や傾向分析が出来るようなログを保管します [対策例] ■稼働状況の確認・記録 AWSの以下のようなサービスを使用し、AWSサービスの稼働状況を確認します。一定期間記録されるため、必要に応じて個別に記録を保持します ・AWSサービス稼働状況：Personal Health Dashboard ・各サービスの稼働状況：CloudWatchメトリクス(稼働確認、記録、ログ保管) ・システムのログ：CloudWatchログ ・API操作ログ：CloudTrail(CloudWatchログに出力を推奨) ■検知 システムに問題がある動きがある場合に、速やかに検出するために、以下機能を設定します ・異常検知機能：CloudWatchアラーム
実73	○	○	[BCP(Business Continuity Plan)；事業継続計画] AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。 [パンデミックへの対応] AWS は、感染症の爆発的な流行の脅威に対して迅速に対応するための準備として、パンデミック対応ポリシーと手順を災害復旧計画に組み込んでいます。関連したリスクに関する軽減のためのストラテジーには、重要なプロセスをリージョン外のリソースに移動するために、どのようにスタッフを配置するかという代替モデルと、重要なビジネス業務をサポートするための危機管理の発動計画が含まれます。パンデミック計画は、国際的な健康関連機関や規制に従っていますが、国際的な関連機関との連絡窓口等も含まれています。 [事業継続性管理] Amazon のインフラストラクチャは高いレベルの可用性を備え、回復機能を持つ IT アーキテクチャを配備する機能を顧客に提供します。AWS のシステムは、お客様への影響を最小限に抑えながらシステムまたはハードウェア障害に耐えられるように設計されています。また、AWS におけるデータセンターの事業の継続性は、Amazon Infrastructure Group の指示に従って管理されます。 [可用性] 世界各地に設置されているデータセンターは、所在地によりリージョンに分けられています。すべてのデータセンターはオンラインでお客様にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。 AWS を使用すると、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理上のリージョン内に、柔軟にインスタンスを配置してデータを保管できます。各アベイラビリティーゾーンは、障害が発生しても他のゾーンに影響を与えないように設計されています。つまり、アベイラビリティゾーンは、代表的な都市のリージョン内で物理的に区切られており、低リスクの氾濫原にあります（具体的な洪水帯の分類はリージョンによって異なります）。個別の無停電電源装置（UPS）やオンサイトのバックアップ生成施設に加え、シングルポイントの障害の可能性を減らすために、別々の電力供給施設から異なる配管網を経由して、個別に電力供給を行っています。アベイラビリティゾーンはすべて、複数の Tier-1 トランジットプロバイダに重複して接続しています。 AWS の使用量は、複数のリージョンやアベイラビリティーゾーンを利用できるように設計することをお勧めします。複数のアベイラビリティゾーンにアプリケーションを配置すると、自然災害やシステム障害を含むほとんどの障害が発生したときに、回復力を持った状態を保つことができます。 [インシデントへの対応] Amazon のインシデント管理チームは、業界標準の診断手順を採用しており、事業に影響を与えるイベント時に解決へと導きます。作業員スタッフが、24 時間 365 日体制でインシデントを検出し、影響と解決方法を管理します。 [役員による全社的検査] Amazon の内部監査グループは、最近になって AWS サービスの復元プランを検査しました。このプランは、上級役員管理チームと取締役の監査委員会のメンバーによっても定期的に検査されています。 [コミュニケーション] AWSは、様々な方法でグローバルレベルの内部コミュニケーションを実施することで、従業員が各自の役割と責任を理解することを手助けし、重要なイベントについて適時伝達しています。これらの方法には、新入社員向けのオリエンテーションとトレーニングプログラム、業績その他についてアップデートを行う定例のマネジメント会議、ビデオ会議、電子メールメッセージ、Amazon イントラネットでの情報の投稿などの電子的手段があります。	[概要] AWSは環境以外に起因する緊急事態への対応も含め、各種認証に準拠した事業継続ポリシーおよび計画を開発、テストしています。 [関連する認証] ・ISO/IEC 27001 -17.1 情報セキュリティ継続	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報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] 金融機関責任範囲での継続性、可用性維持のコンティンジェンシープランに加え、サイバー攻撃、内部犯行、過失等を想定した機密性(情報漏洩)、完全性(情報改竄)を損ねるケースでのコンティンジェンシープランの策定が必要です。 また、クラウド事業者に対して内部犯行、過失、サイバー攻撃されることを前提としたコンティンジェンシープランの有無を確認されることを推奨します。
実74	○	○	・世界各地に設置されているデータセンターは、所在地によりリージョンに分けられています。すべてのデータセンターはオンラインでお客様にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。 AWS を使用すると、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理上のリージョン内に、柔軟にインスタンスを配置してデータを保管できます。各アベイラビリティーゾーンは、障害が発生しても他のゾーンに影響を与えないように設計されています。つまり、アベイラビリティゾーンは、代表的な都市のリージョン内で物理的に区切られており、低リスクの氾濫原にあります（具体的な洪水帯の分類はリージョンによって異なります）。個別の無停電電源装置（UPS）やオンサイトのバックアップ生成施設に加え、シングルポイントの障害の可能性を減らすために、別々の電力供給施設から異なる配管網を経由して、個別に電力供給を行っています。アベイラビリティゾーンはすべて、複数の Tier-1 トランジットプロバイダに重複して接続しています。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	[概要] ・想定災害とシステム重要度を鑑みて適切なマルチAZ構成やマルチリージョンの構成をとります。 [対策例] ・単一のDC障害を想定する場合：マルチAZ構成になるようシステムを構成することが有効です。 ・広域災害(例：関東領域が使えない)を想定する場合：マルチリージョン構成になるようシステムを構成します。 [参考文献、参考URL] https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/plan-for-disaster-recovery-dr.html
実75	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実76	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実77	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実78	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実79	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実80	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実81	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実82	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実83	-	○	-	[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。 [対処例] 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、統制により具体的なセキュリティが実現されています。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、および破棄 (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。AWSで扱われるメディアはワイプ処理もしくは消磁処理され、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。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/	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報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] システム廃棄時の情報漏洩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、および破棄 (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] 金融機関の責任において、AWS上で論理的に情報を削除してください。 AWSでは、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、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おり、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。AWSで扱われるメディアはワイプ処理もしくは消磁処理され、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。 [参考文献、参考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/
実84	○	○	・Amazon のインフラストラクチャは高いレベルの可用性を備え、回復機能を持つ IT アーキテクチャを配備する機能を顧客に提供します。AWS のシステムは、お客様への影響を最小限に抑えながらシステムまたはハードウェア障害に耐えられるように設計されています。また、AWS におけるデータセンターの事業の継続性は、Amazon Infrastructure Group の指示に従って管理されます。 ・世界各地に設置されているデータセンターは、所在地によりリージョンに分けられています。すべてのデータセンターはオンラインでお客様にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 クラウド環境においてはハードウェアの冗長化のみならず、ソフトウェアによるサービスの冗長化構成も高可用性を実現するために重要な要素となります。 AWS は、堅牢な継続性計画を実装する機能をお客様に提供しています。たとえば、頻繁なサーバーインスタンスバックアップの利用、データの冗長レプリケーション、マルチリージョン/アベイラビリティーゾーンのデプロイアーキテクチャなどです。 また、お客様はAmazon EC2 Auto Scalingを使用することができます。Amazon EC2 Auto Scaling は、Amazon EC2 のインスタンスを自動的に作成または終了してアプリケーションの負荷を処理する Amazon EC2 インスタンスの数を調整できる、完全マネージド型サービスです。Amazon EC2 Auto Scaling では、異常なインスタンスを検出して置き換えることにより、EC2 インスタンスのフリートを管理できます。また、お客様が定義する条件に応じて Amazon EC2 のキャパシティーのスケールアップ/スケールダウンを自動的に行って、アプリケーションの可用性を維持できます。	-
実85	○	○	・Amazon のインフラストラクチャは高いレベルの可用性を備え、回復機能を持つ IT アーキテクチャを配備する機能を顧客に提供します。AWS のシステムは、お客様への影響を最小限に抑えながらシステムまたはハードウェア障害に耐えられるように設計されています。また、AWS におけるデータセンターの事業の継続性は、Amazon Infrastructure Group の指示に従って管理されます。 ・世界各地に設置されているデータセンターは、所在地によりリージョンに分けられています。すべてのデータセンターはオンラインでお客様にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 クラウド環境においてはハードウェアの冗長化のみならず、ソフトウェアによるサービスの冗長化構成も高可用性を実現するために重要な要素となります。 AWS は、堅牢な継続性計画を実装する機能をお客様に提供しています。たとえば、頻繁なサーバーインスタンスバックアップの利用、データの冗長レプリケーション、マルチリージョン/アベイラビリティーゾーンのデプロイアーキテクチャなどです。	-
実86	○	○	・Amazon のインフラストラクチャは高いレベルの可用性を備え、回復機能を持つ IT アーキテクチャを配備する機能を顧客に提供します。AWS のシステムは、お客様への影響を最小限に抑えながらシステムまたはハードウェア障害に耐えられるように設計されています。また、AWS におけるデータセンターの事業の継続性は、Amazon Infrastructure Group の指示に従って管理されます。 ・世界各地に設置されているデータセンターは、所在地によりリージョンに分けられています。すべてのデータセンターはオンラインでお客様にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 クラウド環境においてはハードウェアの冗長化のみならず、ソフトウェアによるサービスの冗長化構成も高可用性を実現するために重要な要素となります。 AWS は、堅牢な継続性計画を実装する機能をお客様に提供しています。たとえば、頻繁なサーバーインスタンスバックアップの利用、データの冗長レプリケーション、マルチリージョン/アベイラビリティーゾーンのデプロイアーキテクチャなどです。	[概要] オンプレミスと同様、特定システムで重要な通信系装置には、障害時の迅速な対応のためオンプレミス環境にネットワーク機器の予備の用意が必須です。 [対策例] ■オンプレミス環境からインターネット経由でAWS環境に接続するケース ・オンプレミス環境にインターネット回線に接続するルータの予備を用意します。 ■オンプレミス環境からVPN経由でAWS環境に接続するケース ・オンプレミス環境にAWS Site to Site VPNを通じてVPNで接続するカスタマーゲートウェイの予備を用意します。 ■オンプレミス環境から専用線経由でAWS環境に接続するケース ・オンプレミス環境にAWS Direct Connectに接続するルータの予備を用意します。 [参考文献、参照URL] ・AWS Site-to-Site VPN とは https://docs.aws.amazon.com/ja_jp/vpn/latest/s2svpn/VPC_VPN.html ・AWS Direct Connect ユーザーガイド https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/Welcome.html

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実87	○	○	各データセンター間は物理的に離れており、冗長性のある電源とネットワーキングを備えています。 AWS ネットワークのインターネット側のそれぞれの境界では、複数の通信サービスへの重複する接続を採用しています。これらの接続にはそれぞれ、専用ネットワークデバイスがあります。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 クラウド環境においてはハードウェアの冗長化のみならず、ソフトウェアによるサービスの冗長化構成も高可用性を実現するために重要な要素となります。 AWS は、堅牢な継続性計画を実装する機能をお客様に提供しています。たとえば、頻繁なサーバーインスタンスバックアップの利用、データの冗長レプリケーション、マルチリージョン/アベイラビリティーゾーンのデプロイアーキテクチャなどです。	[概要] オンプレミスと同様、特定システムの重要な回線には回線障害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。 [対策例] システム構成と要件により、以下の2本目の回線を用意します。 ・インターネットで接続する回線 ・AWS Site to Site VPNで接続する回線 ・AWS Direct Connectで接続する回線 [参考文献、参照URL] ・AWS Site-to-Site VPN とは https://docs.aws.amazon.com/ja_jp/vpn/latest/s2svpn/VPC_VPN.html ・AWS Direct Connect の回復性に関する推奨事項 Direct Connect のバックアップとしての AWS マネージド VPN 接続 https://aws.amazon.com/jp/directconnect/resiliency-recommendation/
実88	○	○	（実87と同様）	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 クラウド環境においてはハードウェアの冗長化のみならず、ソフトウェアによるサービスの冗長化構成も高可用性を実現するために重要な要素となります。 AWS は、堅牢な継続性計画を実装する機能をお客様に提供しています。たとえば、頻繁なサーバーインスタンスバックアップの利用、データの冗長レプリケーション、マルチリージョン/アベイラビリティーゾーンのデプロイアーキテクチャなどです。	-
実89	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実90	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実91	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実92	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実93	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実94	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実95	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実96	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実97	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実98	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実99	○	○	・AWSは幅広く包括的なセキュリティ基準に準拠し、安全な環境を維持するためのベストプラクティスに従っており、 ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 ・Amazon の法人アプリケーションチームは、ソフトウェアの開発と管理を行って、サードパーティのソフトウェア配布、内部開発ソフトウェアと設定管理の領域で、UNIX/Linux ホストの IT プロセスを自動化します。インフラストラクチャチームは、UNIX/Linux 設定管理フレームワークを運用して、ハードウェアの拡張性、可用性、監査、セキュリティ管理を解決します。変更管理の自動プロセスを使用した集中管理ホストにより、当社は、高可用性、再現性、拡張性、セキュリティおよび障害復旧という目標を達成することが可能となります。システムおよびネットワークエンジニアは、これらの自動ツールのステータスを日常的にモニタリングしており、レポートを検証して、設定やソフトウェアの取得または更新に失敗するホストへの対応を行っています。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 AWS Systems Manager を使用することで、複数の AWS のサービスの運用データを一元化し、AWS リソース全体のタスクを自動化できます。アプリケーション、アプリケーションスタックのさまざまなレイヤー、本番環境と開発環境といったリソースの論理グループを作成できます。Systems Manager では、リソースグループを選択し、その最新の API アクティビティ、リソース設定の変更、関連する通知、運用アラート、ソフトウェアインベントリ、パッチコンプライアンス状況を表示できます。運用ニーズに応じて、各リソースグループに対してアクションを実行することもできます。Systems Manager により、AWS リソースを一元的に表示および管理でき、運用を完全に可視化して制御できます。 ・AWS CloudFormation は、開発や本運用に必要な、互いに関連する AWS およびサードパーティのリソースコレクションを作成し、そのリソースを適切な順序でプロビジョニングするためのサービスです。AWS CloudFormation を使用すれば、アプリケーションを駆動する関連リソースのグループを予測可能な方法で繰り返し作成する作業を自動化および簡素化できます。	[概要] オペレーションの自動化、簡略化を図る必要があります。 [対策例] オペレーションの自動化、簡略化のためにAWSは、さまざまなサービスを提供しており、お客様にてサービスを活用していただくことで、自動化、簡略化を図ることができます。 AWS Systems Managerでは、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、運用を完全に可視化して制御できます。 AWS CloudFormationでは、アプリケーションを駆動する関連リソースのグループを予測可能な方法で繰り返し作成する作業を自動化および簡素化できます。 AWS Step Functionsでは、障害、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に想定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処できます。 Amazon EventBridgeでは、イベントの取り込み、フィルタリング、変換、および配信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て、イベントバスから検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 FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実100	○	○	・AWSは幅広く包括的なセキュリティ基準に準拠し、安全な環境を維持するためのベストプラクティスに従っており、 ISO/IEC 27001 への準拠の認定を受けています。これらの認定は独立した第三者監査人によって行われています。 ・AWSにおける変更は、通常、影響が最も少ない領域から段階的な展開で運用環境にプッシュされます。 導入は単一のシステムでテストされ、影響を評価できるよう、綿密に監視されます。 サービス所有者は、サービスのアップストリーム依存関係の健全性を測定する設定可能なメトリックを多数持っています。 これらのメトリックスは、しきい値とアラームが所定の位置に密接に監視されます。 ロールバック手順は、変更管理 (CM) チケットに記載されています。 可能な場合、変更は通常の変更ウィンドウ中にスケジュールされます。 標準の変更管理手順からの逸脱を必要とする本番システムへの緊急の変更は、インシデントに関連付けられ、必要に応じてログに記録され、承認されます。 AWS は、重要なサービスの変更に対する自己監査を定期的に行っており、品質をモニタリングしながら高い基準を維持することによって、変更管理プロセスの継続的な改善に貢献しています。例外は分析され、根本的な原因が決定されて適切な措置が取られます。変更はコンプライアンスに従うようにされるか、または必要に応じてロールバックされます。その後プロセスまたは人的問題を解決して修正するための措置が取られます。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実101	○	○	AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティーに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティープランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 Amazon CloudWatch は、AWS クラウドリソースと AWS で実行されるアプリケーションのモニタリングサービスです。お客様は、Amazon CloudWatch を使用して、メトリクスを収集/追跡し、ログファイルを収集してモニタリングし、アラームを設定できます。Amazon CloudWatch は、Amazon EC2 インスタンス、Amazon DynamoDB テーブル、Amazon RDS DB インスタンスなどの AWS リソース、アプリケーションやサービスに生成されたカスタムメトリクス、アプリケーションが生成するあらゆるログファイルをモニタリングできます。Amazon CloudWatch を使用して、リソース使用率、アプリケーションパフォーマンス、オペレーションの状態においてシステム全体の可視性を得られます。	[概要] 各種AWSリソースの監視の結果や、運用上発生するイベント(キャンペーンで対顧アクセス増加が見込まれる場合等)によるキャパシティ要求の変化に応じて制御を行います。 上記の設定によって、SLAや限界性能を満たせることをテストします。 [対策例] ■監視（「お客様が統制すべき内容」に記載されていないもの） ・分析を行う場合はAmazon CloudWatchだけでなくS3バケットにもログを保存し、Amazon Athena, AWS Glue, Amazon OpenSearch Service等を活用できます。 ・オンプレミスやクラウド、SaaSとの統合管理が必要な場合はサードパーティ製品の利用も検討します。 ■制御 ・EC2等を利用の場合は負荷状況に応じた Auto Scalingを構成します。 → サービスクォータ (リソース起動数等の制限) の引き上げ要否・可否に留意します。 → アクセス経路上の各種サービス (Elastic Load Balancerなど) のスケーラビリティにも留意します。 ・突発的なアクセス上昇が見込まれる場合は予め各種リソースをスケールさせておきます。 → ALB/CLBの拡張が間に合わない程度の急騰であれば暖気(Pre-Warming)申請を行う必要がある点に留意します。 [参考文献、参照URL] https://wa.aws.amazon.com/wat.pillar.reliability.ja.html https://docs.aws.amazon.com/ja_jp/autoscaling/application/userguide/what-is-application-auto-scaling.html https://docs.aws.amazon.com/ja_jp/general/latest/gr/aws_service_limits.html https://aws.amazon.com/jp/blogs/news/webinar-bb-elastic-load-balancing-2019/ ※資料52ページに暖気申請について言及されています
実102	○	○	AWS は、様々な自動モニタリングシステムを活用して、ハイレベルなサービスパフォーマンスと可用性を提供します。 AWS モニタリングツールは、異常な、または不正なアクティビティと条件を通信の出入り口で検出するように設計されています。これらのツールは、サーバーおよびネットワークの利用状況、ポートスキャニングアクティビティ、アプリケーションの利用状況、および許可されていない侵入の試みをモニタリングします。このツールを使用して、異常なアクティビティに対して独自に性能測定基準のしきい値を設定することができます。 AWS 内のシステムには膨大な装置が備わっており、主要なオペレーションメトリックをモニタリングしています。主要なオペレーションメトリックが早期警告しきい値を超えた場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。オンコールスケジュール（常時待機体制）が採用されているので、担当者が運用上の問題にいつでも対応することができます。	[概要] AWSのデータセンターが備えている運用状況の監視機能については、SOC 2 type Ⅱレポートにて明記されている。 [関連する認証] ・SOC 2 type Ⅱレポート -SECTION III - Relevant Aspects of Internal Controls -E. Monitoring	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 Amazon CloudWatch は、AWS クラウドリソースと AWS で実行されるアプリケーションのモニタリングサービスです。お客様は、Amazon CloudWatch を使用して、メトリクスを収集/追跡し、ログファイルを収集してモニタリングし、アラームを設定できます。Amazon CloudWatch は、Amazon EC2 インスタンス、Amazon DynamoDB テーブル、Amazon RDS DB インスタンスなどの AWS リソース、アプリケーションやサービスに生成されたカスタムメトリクス、アプリケーションが生成するあらゆるログファイルをモニタリングできます。Amazon CloudWatch を使用して、リソース使用率、アプリケーションパフォーマンス、オペレーションの状態においてシステム全体の可視性を得られます。	[概要] AWS上で構築・運用するシステムでは監視対象として以下が追加となるため、これらに対する監視手段を検討し、実装する必要があります。 (1) AWSリソース(例：EC2インスタンスのステータス、Lambda関数の実行状況等)の稼働状態 (2) AWSサービス自体の稼働状態 [対策例] (1) AWSリソース(例：EC2インスタンスのステータス、Lambda関数の実行状況等)自体を監視する手段として、AWSの各種監視用のサービス(Amazon CloudWatch等)が活用できます。(※1) (2) また、各AWSサービス自体の稼働状態を監視する手段として、AWS Service Health Dashboard、AWS Personal Health Dashboard等があり、それらの情報を活用することができます。(※2)(※3) なお、OS以上のレイヤで施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。 [参考文献、参照URL] (※1)Amazon CloudWatch ユーザーガイド ・Amazon CloudWatch とは https://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html (※2)AWS Health ユーザーガイド ・AWS Health のセキュリティのベストプラクティス https://docs.aws.amazon.com/ja_jp/health/latest/ug/security-best-practices.html (※3)AWS Service Health Dashboard https://status.aws.amazon.com/

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実103	○	○	AWS は、様々な自動モニタリングシステムを活用して、ハイレベルなサービスパフォーマンスと可用性を提供します。 AWS モニタリングツールは、異常な、または不正なアクティビティと条件を通信の出入り口で検出するように設計されています。これらのツールは、サーバーおよびネットワークの利用状況、ポートスキャニングアクティビティ、アプリケーションの利用状況、および許可されていない侵入の試みをモニタリングします。このツールを使用して、異常なアクティビティに対して独自に性能測定基準のしきい値を設定することができます。 AWS 内のシステムには膨大な装置が備わっており、主要なオペレーションメトリックをモニタリングしています。主要なオペレーションメトリックが早期警告しきい値を超えた場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。オンコールスケジュール（常時待機体制）が採用されているので、担当者が運用上の問題にいつでも対応することができます。	[概要] AWSのデータセンタが備えている障害の検出及び障害箇所の切り分け機能について、直接言及している公開情報は無い。しかし本機能を備えることの目的は、障害発生時の迅速な復旧を実現することであり、AWSが左記を実現するために実施している対策はSOC 2 type Ⅱレポートから読み取ることが可能である。 [関連する認証] ・SOC 2 type Ⅱレポート -SECTION III - Relevant Aspects of Internal Controls -D.8 Data Integrity, Availability, and Redundancy	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。 Amazon CloudWatch は、AWS クラウドリソースと AWS で実行されるアプリケーションのモニタリングサービスです。お客様は、Amazon CloudWatch を使用して、メトリクスを収集/追跡し、ログファイルを収集してモニタリングし、アラームを設定できます。Amazon CloudWatch は、Amazon EC2 インスタンス、Amazon DynamoDB テーブル、Amazon RDS DB インスタンスなどの AWS リソース、アプリケーションやサービスに生成されたカスタムメトリクス、アプリケーションが生成するあらゆるログファイルをモニタリングできます。Amazon CloudWatch を使用して、リソース使用率、アプリケーションパフォーマンス、オペレーションの状態においてシステム全体の可視性を得られます。	[概要] AWS上で構築・運用するシステムでは障害が発生しうるポイントとして以下が追加となるため、これらに対する監視手段を検討し、実装する必要があります。 (1) AWSリソース(例：EC2インスタンスのステータス、Lambda関数の実行状況等) (2) AWSサービス自体 [対策例] (1) AWSリソース(例：EC2インスタンスのステータス、Lambda関数の実行状況等)の異常を検出する手段として、AWSの各種監視用のサービス(CloudWatch等)が活用できます。(※1) (2) また、各AWSサービス自体の異常を検出する手段として、AWS Service Health Dashboard、AWS Personal Health Dashboard等があり、それらの情報を活用することができます。(※2)(※3) なお、OS以上のレイヤで施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。 [参考文献、参照URL] (※1)Amazon CloudWatch ユーザーガイド ・Amazon CloudWatch とは https://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html (※2)AWS Health ユーザーガイド ・AWS Health のセキュリティのベストプラクティス https://docs.aws.amazon.com/ja_jp/health/latest/ug/security-best-practices.html (※3)AWS Service Health Dashboard https://status.aws.amazon.com/
実104	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	[概要] 障害発生時に備えて再構成の機能を利用します。再構成は可能な限り自動化します。 要件によってはマルチAZやマルチリージョンの構成も検討します。障害発生時を想定したテストを実施します。 [対策例] ・各種障害を検知するための監視を構成します。 ・各リソースの高可用性設計に応じてクラスタリングを構成します。 ・EC2等を利用の場合は負荷状況に応じたAuto Scalingを構成します。 → ステートフルなシステムの場合はAZ障害後の自動再構成時に、スケーリングプロセス「AZRebalance」の取扱いに留意します。 (注)AZが復旧した際にAZごとのリソース数をリバランスされるため、自動再構成されたリソースが再度Terminateされる恐れがあります。 ・EC2を利用の場合はAWS管理の物理ホストでの障害に備え、Auto Recoveryを有効化します。 [参考文献、参照URL] https://wa.aws.amazon.com/wat.pillar.reliability.ja.html
実105	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実106	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	[概要] 障害発生時に備えて再構成やバックアップの機能を利用します。いずれも可能な限り自動化します。 あらかじめ定められた目標復旧時間 (RTO) と目標復旧時点 (RPO)に従って設定し、リカバリテストを実施します。 [対策例] ((注)実104に記載の対策は省略) ・AWS Backup によるバックアップの集中管理を実施します。 → 自動でリストアされない項目については、別途作り込みもしくは手動でのリストアが必要である点に留意します。 ・要件によって、クロスリージョンバックアップ構成を検討します。 [参考文献、参照URL] https://wa.aws.amazon.com/wat.pillar.reliability.ja.html https://aws.amazon.com/jp/backup/
実107	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実108	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実109	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実110	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実111	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実112	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実113	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実114	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

「AWS FISC安全対策基準対応リファレンス」からの引用				参考情報	「AWS FISC安全対策基準対応リファレンス」からの引用	参考情報
基準番号	対応の主体		AWSの対応状況		お客様が統制すべき内容	
	AWS	お客様				
実115	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実116	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実117	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実118	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実119	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実120	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実121	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実122	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実123	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実124	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実125	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実126	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実127	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実128	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実129	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実130	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実131	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実132	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実133	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実134	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実135	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実136	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実137	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実138	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実139	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実140	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-
実141	-	○	-	-	お客様がAWS上で実装するシステムおよびサービスの管理は、AWSが提供する機能および情報もしくはその他の機能を用いて、お客様にて実施します。	-

「AWS FISC安全対策基準対応リファレンス」からの引用					付加情報
基準番号	枝番	対応の主体		AWSの対応状況	
		AWS	お客様		
監1	1	-	○	・以下の情報を参考にAWSを外部委託先としての監査にお役立てください。 従来、統制目標と統制の設計と運用効率の検証は、社内外の監査人がプロセスを実地検証し、証拠を評価することによって行われています。お客様またはお客様の社外監査人による直接の監視または検証は、一般的に、統制の妥当性を確認するために行われます。AWS などのサービスプロバイダーを使用する場合、企業はサードパーティーによる証明および認定を要求し、評価することで、統制目標と統制の設計と運用効率の合理的な保証を獲得します。その結果、お客様の主な統制を AWS が管理している場合でも、統制環境を統一されたフレームワークのまま維持し、効率的に運用しながらすべての統制を把握し、検証することができます。サードパーティーによる証明と AWS の認定によって、統制環境を高いレベルで検証できるだけでなく、AWS クラウドの自社の IT 環境に対して特定の検証作業を自社で実行する要求を持つお客様にも役立ちます。 AWS にデプロイされている部分では、AWS が該当する物理コンポーネントを統制します。その他の部分は、接続ポイントや送信の統制を含め、お客様がすべてを所有し、統制することになります。AWS で定めている統制の内容と、その統制がどのように効果的に運用されているかについて、AWS では SOC1 Type II レポートを発行し、EC2、S3、VPC などに関連し定義された統制、ならびに詳細な物理セキュリティおよび環境に関する統制を公表しています。これらの統制は、ほとんどのお客様のニーズに見合うように、ハイレベルで定義されています。AWS と機密保持契約を結んでいる AWS のお客様は、SOC1 Type II レポートを要求できます。 ほとんどのレイヤーと、物理統制よりも上の統制の監査は、お客様の責任範囲となります。AWS の論理統制と物理統制の定義は、SOC 1 Type II レポートに文書化されています。このレポートはお客様の監査チームとコンプライアンスチームのレビューに使用できます。また、AWS ISO/IEC 27001 およびその他の認定も監査人のレビュー用に使用できます。	[概要] 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。 [参考文献、参照URL] ・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	-	○	・以下の情報を参考にAWSを外部委託先としての監査にお役立てください。 従来、統制目標と統制の設計と運用効率の検証は、社内外の監査人がプロセスを実地検証し、証拠を評価することによって行われています。お客様またはお客様の社外監査人による直接の監視または検証は、一般的に、統制の妥当性を確認するために行われます。AWS などのサービスプロバイダーを使用する場合、企業はサードパーティーによる証明および認定を要求し、評価することで、統制目標と統制の設計と運用効率の合理的な保証を獲得します。その結果、お客様の主な統制を AWS が管理している場合でも、統制環境を統一されたフレームワークのまま維持し、効率的に運用しながらすべての統制を把握し、検証することができます。サードパーティーによる証明と AWS の認定によって、統制環境を高いレベルで検証できるだけでなく、AWS クラウドの自社の IT 環境に対して特定の検証作業を自社で実行する要求を持つお客様にも役立ちます。	[概要] AWS上に存在する情報の取扱いは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。 [参考文献、参照URL] ・責任共有モデル https://aws.amazon.com/jp/compliance/shared-responsibility-model/
	4	-	○	・以下の情報を参考にAWSを外部委託先としての監査にお役立てください。 ほとんどのレイヤーと、物理統制よりも上の統制の監査は、お客様の責任範囲となります。AWS の論理統制と物理統制の定義は、SOC 1 Type II レポートに文書化されています。このレポートはお客様の監査チームとコンプライアンスチームのレビューに使用できます。また、AWS ISO/IEC 27001 およびその他の認定も監査人のレビュー用に使用できます。 事実確認および意見交換等に関するお問い合わせは担当営業までご連絡ください。	[概要] 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。 [参考文献、参照URL] ・『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	-	○	・以下の情報を参考にAWSを外部委託先としての監査にお役立てください。 AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、当社の IT 統制環境に関する幅広い情報をお客様にご提供しています。本文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様にご理解いただくことをお手伝いするためのものです。この情報はまた、お客様の拡張された IT 環境内の統制が効果的に機能しているかどうかを明らかにし、検証するのにも有用です。 従来、統制目標と統制の設計と運用効率の検証は、社内外の監査人がプロセスを実地検証し、証拠を評価することによって行われています。お客様またはお客様の社外監査人による直接の監視または検証は、一般的に、統制の妥当性を確認するために行われます。AWS などのサービスプロバイダーを使用する場合、企業はサードパーティーによる証明および認定を要求し、評価することで、統制目標と統制の設計と運用効率の合理的な保証を獲得します。その結果、お客様の主な統制を AWS が管理している場合でも、統制環境を統一されたフレームワークのまま維持し、効率的に運用しながらすべての統制を把握し、検証することができます。サードパーティーによる証明と AWS の認定によって、統制環境を高いレベルで検証できるだけでなく、AWS クラウドの自社の IT 環境に対して特定の検証作業を自社で実行する要求を持つお客様にも役立ちます。 AWS のデータセンターは複数のお客様をホストしており、幅広いお客様が第三者による物理的なアクセスの対象となるため、お客様によるデータセンター訪問は許可していません。このようなお客様のニーズを満たすために、SOC 1 Type II レポートの一環として、独立し、資格を持つ監査人が統制の有無と運用を検証しています。この広く受け入れられているサードパーティーによる検証によって、お客様は実行されている統制の効果について独立した観点を得ることができます。AWS と機密保持契約を結んでいる AWS のお客様は、SOC 1 Type II レポートのコピーを要求できます。データセンターの物理的なセキュリティの個別の確認も、ISO/IEC 27001 監査、PCI 評価、ITAR 監査、FedRAMP テストプログラムの一部となっています。	[概要] ・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。 ※SOCレポートの利用に際しては、統26-3も参照 [参考文献、参照URL] ・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 https://aws.amazon.com/jp/compliance/sub-processors/