金融機関向け AWS FISC安全対策基準対応リファレンス

金融情報システムセンター（FISC）「金融機関等コンピュータシステムの安全対策基準・解説書 第9版 （令和3年12月版）」対応

2022年5月

作成： アマゾン ウェブ サービス ジャパン合同会社

【はじめに】
お客様が、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際の参考情報として、FISC安全対策基準（第9版 令和2年3月版）「統制基準」「実務基準」「監査基準」に沿って整理しています。

【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（お客様のコンピューターセンター・共同センター、本部・営業店等）やお客様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）、FISC安全対策基準の「設備基準」は本リファレンスの対象外とします。

【本リファレンスの見方】
<対応の主体>
「AWS（クラウド事業者）」ならびに「お客様（利用者）」のそれぞれが主体として対応する項目欄に”○”、必要に応じて情報を提供する項目を”－”としています。
AWSおよびお客様の両者が主体として対応する場合は両方を”○”としています。

<AWSの対応状況>
AWSの対応方針やAWSの提供しているソリューションについて記載しています。

＜補足情報＞
参照が可能なAWSのホワイトペーパー等の公開情報について記載しました。PCI DSS およびISO/IEC 27000シリーズの項目番号については、特に指定のない場合は以下のバージョンに基づき記載しております。
・PCI DSS v3.2，ISO/IEC 27001:2013, ISO/IEC 27002:2013

【責任共有モデルとは】
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となります（責任共有モデル）。
責任共有モデルの詳細については、https://aws.amazon.com/jp/compliance/shared-responsibility-model/ を参照ください。

【金融機関等コンピュータシステムの安全対策基準・解説書の著作権】
「金融機関等コンピュータシステムの安全対策基準・解説書」は公益財団法人 金融情報システムセンターの著作物です。本リファレンスへの基準番号 項番の記載については公益財団法人 金融情報システムセンターの許可を得ております。

【免責事項】
本文書は情報提供のみを目的としています。本文書は、発行時点における AWS の製品と対応を説明するものであり、予告なく変更される場合があります。お客様は、本文書の情報および AWS 製品またはサービスの利用について、ご自身の評価に基づき判断する責任を負います。いずれの AWS 製品またはサービスも、明示または黙示を問わずいかなる保証も伴うことなく、「現状のまま」提供されます。本文書のいかなる内容も、AWS とその関係会社、サプライヤー、またはライセンサーからの保証、表明、および契約上の責任、条件や確約を意味するものではありません。お客様に対する AWS の責任は AWS 契約によって規定されています。また、本文書は、AWS とお客様との間のいかなる契約の一部も構成するものではなく、また、当該契約が本文書によって変更されることもありません。

ISO/IEC 27001:2013

ISO/IEC 27002 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制御を規定したセキュリティ管理標準です。この認証の基礎は強固なセキュリティプログラムの開発と実装であり、これには、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する、情報セキュリティ管理システム (ISMS) の開発と実装が含まれます。この広く認められている国際的なセキュリティ標準によると、AWS は次のことを実行する必要があります。

- 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。
- 一連の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ーのセキュリティリスクに対処する。
- 情報セキュリティ統制がニーズを継続的に満たすことを確実にするために、包括的な管理プロセスを採用する。

AWS は ISO/IEC 27001:2013、27017:2015、および 27018:2014 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ます。このように国際的に認められた規格および実施基準に準拠しているということは、AWS が組織のすべてのレベルで情報セキュリティに取り組んでいること、および AWS のセキュリティプログラムが業界の主なベストプラクティスに従っていることの証拠です。

最新、詳細情報は下記のサイトを参照ください。
https://aws.amazon.com/jp/compliance/iso-27001-faqs/

SOCレポート

AWS System & Organization Control (SOC) レポートは、重要なコンプライアンス管理および目標を AWS がどのように達成したかを実証する、独立したサードパーティーによる審査報告書です。このレポートの目的は、お客様とお客様の監査人が、オペレーションとコンプライアンスをサポートするよう確立された AWS 統制を簡単に把握できるようにすることです。

SOC 1：AWS の統制環境に関する説明、および AWS が定義した統制と目標の外部監査に関する説明
SOC 2：セキュリティ、可用性、機密性 - AWS の統制環境に関する説明と AICPA の信頼サービスのセキュリティ、可用性、機密性の原則および基準を満たす AWS 統制の外部監査に関する説明
SOC 2：プライバシー - AWS の統制環境に関する説明と AICPA の信頼サービスのセキュリティ、可用性、機密性の原則および基準を満たす AWS 統制の外部監査に関する説明
SOC 3：セキュリティ、可用性、機密性:AWS が AICPA の信頼サービスのセキュリティ、可用性、機密性の原則および基準を満たしていることを実証する公開レポート

最新、詳細情報は下記のサイトを参照ください。

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
-	-	-	-	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。	-
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	-	○	-	-

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
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/	-

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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。	

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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/ 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/	

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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/	

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
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/	-

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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)	-	○	-	-

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
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。	-

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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/	

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
統20	3-(5)	-	○	AWSの補助処理者、下請け業者に関する情報は以下のサイトをご参照ください。 AWS の補助処理者: https://aws.amazon.com/jp/compliance/sub-processors/ 下請け業者のアクセス: https://aws.amazon.com/jp/compliance/third-party-access/	-
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。	-

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
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/	-

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
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/	-
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/	-

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
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	-
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的および物理的な管理を実践しています。 https://aws.amazon.com/jp/compliance/data-privacy-faq/ 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/	-

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
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的および物理的な管理を実践しています。 https://aws.amazon.com/jp/compliance/data-privacy-faq/	-
統20	3-(13)	-	○	・AWS では 200 種類を超えるクラウドサービスについて従量制料金を適用しています。 AWS では必要な個々のサービスにのみ、サービスを使用する期間だけお支払いいただき、長期契約や複雑なライセンスは必要ありません。 サービスを消費した分だけ支払い、サービスの使用を停止したときの追加コストや解約料金はありません。 https://aws.amazon.com/jp/pricing/	-
統20	3-(14)		○	・AWSのカスタマーアグリーメントにおいて、クラウドサービスの販売者がアマゾン ウェブ サービス ジャパン合同会社のアカウントについては「準拠法」を日本国法、「管轄裁判所」を東京地裁と定めています。	
統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 ・AWSのカスタマーアグリーメントにおいて、クラウドサービスの販売者がアマゾン ウェブ サービス ジャパン合同会社のアカウントについては「準拠法」を日本国法、「管轄裁判所」を東京地裁と定めています。	-
統21	3	-	○	-	-

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
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。	-

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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、可用性をアクセスするとともに、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。 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/	

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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。	-

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
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/	-
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。	-

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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/	

注意: 本文書は情報提供のみを目的としています。本文書は、発行時点における AWS の製品と対応を説明するものであり、予告なく変更される場合があります。お客様は、本文書の情報および AWS 製品またはサービスの利用について、ご自身の評価に基づき判断する責任を負います。いずれの AWS 製品またはサービスも、明示また は黙示を問わずいかなる保証も伴うことなく、「現状のまま」提供されます。本文書のいかなる内容も、AWS とその関係会社、サプライヤー、またはライセンサーからの保証、表明、および契約上の責任、条件や確約を意味するものではありません。お客様に対する AWS の責任は AWS 契約によって規定されています。また、本文書は、 AWS とお客様との間のいかなる契約の一部も構成するものではなく、また、当該契約が本文書によって変更されることもありません。

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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	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	-

注意: 本文書は情報提供のみを目的としています。本文書は、発行時点における AWS の製品と対応を説明するものであり、予告なく変更される場合があります。お客様は、本文書の情報および AWS 製品またはサービスの利用について、ご自身の評価に基づき判断する責任を負います。いずれの AWS 製品またはサービスも、明示また は黙示を問わずいかなる保証も伴うことなく、「現状のまま」提供されます。本文書のいかなる内容も、AWS とその関係会社、サプライヤー、またはライセンサーからの保証、表明、および契約上の責任、条件や確約を意味するものではありません。お客様に対する AWS の責任は AWS 契約によって規定されています。また、本文書は、 AWS とお客様との間のいかなる契約の一部も構成するものではなく、また、当該契約が本文書によって変更されることもありません。

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				・AWSのカスタマーアグリーメントにおいて、クラウドサービスの販売者がアマゾン ウェブ サービス ジャパン合同会社のアカウントについては「準拠法」を日本国法、「管轄裁判所」を東京地裁と定めています。 ・AWS 環境にデプロイしたインフラストラクチャの統制に関して AWS にデプロイされている部分では、AWS が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。	

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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/	

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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	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	-

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				・AWSのカスタマーアグリーメントにおいて、クラウドサービスの販売者がアマゾン ウェブ サービス ジャパン合同会社のアカウントについては「準拠法」を日本国法、「管轄裁判所」を東京地裁と定めています。 ・AWS 環境にデプロイしたインフラストラクチャの統制に関して AWS にデプロイされている部分では、AWS が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。	

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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。	

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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。	

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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/	

注意: 本文書は情報提供のみを目的としています。本文書は、発行時点における AWS の製品と対応を説明するものであり、予告なく変更される場合があります。お客様は、本文書の情報および AWS 製品またはサービスの利用について、ご自身の評価に基づき判断する責任を負います。いずれの AWS 製品またはサービスも、明示また は黙示を問わずいかなる保証も伴うことなく、「現状のまま」提供されます。本文書のいかなる内容も、AWS とその関係会社、サプライヤー、またはライセンサーからの保証、表明、および契約上の責任、条件や確約を意味するものではありません。お客様に対する AWS の責任は AWS 契約によって規定されています。また、本文書は、 AWS とお客様との間のいかなる契約の一部も構成するものではなく、また、当該契約が本文書によって変更されることもありません。

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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/	

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
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。	-

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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。	

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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/	

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
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	-

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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。	

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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/	

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
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/	-

注意: 本文書は情報提供のみを目的としています。本文書は、発行時点における AWS の製品と対応を説明するものであり、予告なく変更される場合があります。お客様は、本文書の情報および AWS 製品またはサービスの利用について、ご自身の評価に基づき判断する責任を負います。いずれの AWS 製品またはサービスも、明示また は黙示を問わずいかなる保証も伴うことなく、「現状のまま」提供されます。本文書のいかなる内容も、AWS とその関係会社、サプライヤー、またはライセンサーからの保証、表明、および契約上の責任、条件や確約を意味するものではありません。お客様に対する AWS の責任は AWS 契約によって規定されています。また、本文書は、 AWS とお客様との間のいかなる契約の一部も構成するものではなく、また、当該契約が本文書によって変更されることもありません。

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
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。	-

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

基準番号	枝番	対応の主体		AWSの対応状況	補足情報
		AWS	お客様		
				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25	-	-	○	-	-
統26	-	-	○	-	-
統27	-	-	○	-	-