主要なコンプライアンス

に関する質問と AWS の回答

2017 年 1 月

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。

目次

要約

このドキュメントでは、AWS に関連するコンプライアンスについてのよくある質問と回答を掲載しています。以下に続く内容は、クラウドコンピューティング環境においてシステムを評価および運用する際に重要となり、AWS のお客様の統制を管理する上で役立つものです。

コンプライアンスに関する質問と回答

カテゴリ	クラウドコンピューティングに関する質問	AWS の情報
統制の所有権	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、誰がどの統制を保有することになりますか？	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 SOC 1 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、SOC 1 Type II レポートを要求できます。
IT の監査	AWS 環境を利用している場合、監査はどのように実施すればよいのでしょうか?	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 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。

カテゴリ	クラウドコンピューティングに関する質問	AWS の情報
Sarbanes-Oxley への準拠	対象のシステムが AWS 環境にデプロイされている場合、SOX への準拠はどのように達成されますか?	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。
HIPAA への準拠	AWS 環境にシステムをデプロイしている場合でも、HIPAA のコンプライアンス要件を満たすことができますか?	HIPAA 要件は AWS のお客様に適用され、AWS のお客様が統制します。AWS プラットフォームでは、HIPAA などの業界固有の認定要件を満たすソリューションのデプロイが可能です。お客様は AWS のサービスを利用することで、電子健康記録を保護するために必要な要件以上のセキュリティレベルを維持できます。HIPAA のセキュリティおよびプライバシーに関する規則に準拠したヘルスケアアプリケーションが、お客様によって AWS 上で構築されています。AWS のウェブサイトには、このトピックに関するホワイトペーパーなど、HIPAA への準拠に関する追加情報が掲載されています。
GLBA への準拠	AWS 環境にシステムをデプロイしている場合でも、GLBA の認定要件を満たすことができますか?	ほとんどの GLBA 要件は、AWS のお客様が統制します。AWS は、データの保護、アクセス許可の管理、および AWS インフラストラクチャでの GLBA 準拠アプリケーションの構築をお客様が行うための手段を提供しています。物理セキュリティ統制が効果的に運用されているかどうか具体的な保証が必要な場合は、必要に応じて AWS SOC 1 Type II レポートを参照できます。

カテゴリ	クラウドコンピューティングに関する質問	AWS の情報
米国連邦規制への準拠	米国政府機関が AWS 環境にシステムをデプロイしている場合に、セキュリティおよびプライバシーの規制に準拠することはできますか?	米国連邦機関は、2002 年施行の連邦情報セキュリティマネジメント法 (FISMA)、Federal Risk and Authorization Management Program (FedRAMP)、Federal Information Processing Standard (FIPS) 出版物 140-2、武器規制国際交渉規則 (ITAR) など、数多くのコンプライアンス基準に準拠することができます。また、該当する法律に規定されている要件に応じて、他の法律や状況への準拠も達成できる場合があります。
データの場所	ユーザーデータはどこにありますか?	データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。S3 データオブジェクトのデータレプリケーションは、データが保存されているリージョンのデータセンタークラスタ内でのみ実行され、他のリージョンの他のデータセンタークラスタにレプリケートされることはありません。データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。AWS は、法律または政府機関の要請の遵守が要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しないものとします。リージョンの完全なリストについては、下記のサイトを参照してください。 https://aws.amazon.com/about-aws/global-infrastructure

カテゴリ	クラウドコンピューティングに関する質問	AWS の情報
E-Discovery	AWS 環境では、顧客の e ディスカバリに関する手順、および要件を満たすことが可能ですか?	AWS はインフラストラクチャを提供し、その他の部分はお客様が管理します。例えば、オペレーティングシステム、ネットワーク構成、インストールされているアプリケーションなどです。お客様は、AWS を使用して保存または処理する電子文書の特定、収集、処理、分析、および作成に関連する法的手続きに、適切に対応する責任を持ちます。法的手続きに AWS の協力を必要とするお客様には、お客様の要請に応じて連携をとることになります。
データセンター訪問	ユーザーによるデータセンター訪問を許可していますか?	いいえ。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 1 Type II レポートのコピーを要求できます。また、データセンターの物理的なセキュリティの個別の確認についても、ISO 27001 監査、PCI 評価、ITAR 監査、FedRAMP[sm] 等のテストプログラムの一部となっています。

カテゴリ	クラウドコンピューティングに関する質問	AWS の情報
サードパーティのアクセス	第三者が AWS のデータセンターにアクセスできますか?	AWS 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。物理的なアクセス、データセンターへのアクセスの承認、その他の関連統制については、SOC 1 Type II レポートを参照してください。
特権的アクション	特権的アクションは監視および統制されていますか?	所定の統制によってシステムとデータのアクセスを制限し、システムまたはデータに対するアクセスを制限および監視可能にしています。さらに、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様とは論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC 1、ISO 27001、PCI、ITAR、および FedRAMP[sm] の監査中に独立監査人によって確認されます。
内部者によるアクセス	ユーザーのデータとアプリケーションに対する内部者による不適切なアクセスの脅威に対処していますか?	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。また、本文書で説明している認定およびコンプライアンスの取り組みにより、内部者によるアクセスに対処しています。すべての認定とサードパーティによる証明で、論理アクセスの予防統制と発見的統制が評価されています。さらに、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。

カテゴリ	クラウドコンピューティングに関する質問	AWS の情報
マルチテナンシー	ユーザーの分離は安全に実施されていますか?	AWS 環境は仮想化されたマルチテナント環境です。AWS は、お客様間を隔離するために設計されたセキュリティ管理プロセス、PCI 統制、その他のセキュリティ統制を実装しています。AWS システムは、仮想化ソフトウェアによるフィルタリング処理により、お客様に割り当てられていない物理ホストや物理インスタンスにアクセスできないように設計されています。このアーキテクチャは独立 PCI 認定審査機関 (QSA) によって検証済みであり、2015 年 4 月に発行された PCI DSS 3.1 版のすべての要件に準拠することが確認されています。 **注意**: また、AWS にはシングルテナントのオプションもあります。ハードウェア専有インスタンスは、単一のお客様専用のハードウェアを実行する Amazon Virtual Private Cloud (Amazon VPC) で起動される Amazon EC2 インスタンスです。ハードウェア専有インスタンスを使用することで、Amazon VPC および AWS クラウドの利点をフルに活用しながら、Amazon EC2 インスタンスをハードウェアレベルで隔離できます。

カテゴリ	クラウドコンピューティングに関する質問	AWS の情報
ハイパーバイザーの脆弱性	ハイパーバイザーの既知の脆弱性に対処していますか?	現在、Amazon EC2 は、高度にカスタマイズされたバージョンの Xen ハイパーバイザーを利用しています。ハイパーバイザーは、社内および社外の侵害対策チームによって新規および既存の脆弱性とアタックベクターについて定期的に評価しています。また、ゲスト仮想マシン間の強力な隔離を維持するためにも適したものとなっています。AWS Xen ハイパーバイザーのセキュリティは、評価および監査の際に独立監査人によって定期的に評価されています。Xen ハイパーバイザーとインスタンスの隔離の詳細については、AWS セキュリティホワイトペーパーをご覧ください。
脆弱性管理	システムには適切にパッチが適用されていますか?	AWS は、ハイパーバイザーおよびネットワーキングサービスなど、お客様へのサービス提供をサポートするシステムにパッチを適用する責任を持ちます。この処理は、AWS ポリシーに従い、また ISO 27001、NIST、および PCI の要件に準拠して、必要に応じて実施されます。お客様が使用しているゲストオペレーティングシステム、ソフトウェア、およびアプリケーションの統制については、お客様がそれらのシステムへのパッチ適用を実施する責任を持ちます。
暗号化	提供されているサービスは暗号化をサポートしていますか?	はい。AWS では、S3、EBS、SimpleDB、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することが許可されています。VPC への IPSec トンネルも暗号化されます。また、Amazon S3 は、お客様向けのオプションとしてサーバー側の暗号化も提供しています。お客様は、サードパーティの暗号化テクノロジを使用することもできます。詳細については、AWS セキュリティホワイトペーパーを参照してください。

カテゴリ	クラウドコンピューティングに関する質問	AWS の情報
データの所有権	ユーザーデータに関する権利はどう考えられますか?	AWS のお客様は、お客様自身のデータの統制と所有権を維持します。AWS はお客様のプライバシー保護を慎重に考慮し、AWS が準拠する必要がある法的処置の要求についても注意深く判断しています。AWS は、法的処置による命令に確実な根拠がないと判断した場合は、その命令にためらわずに異議を申し立てます。
データの隔離	ユーザーデータを適切に隔離していますか?	AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。Amazon S3 は高度なデータアクセス統制を提供しています。具体的なデータサービスのセキュリティの詳細については、AWS セキュリティホワイトペーパーをご覧ください。
複合サービス	他のプロバイダーのクラウドサービスをベースに利用し、サービスを提供していますか?	AWS はお客様に AWS のサービスを提供するにあたり、サードパーティのクラウドプロバイダーは一切使用していません。
物理統制と環境統制	統制は、AWS によって運営されていますか?	はい。該当の統制は、SOC 1 Type II レポートに具体的に記載されています。さらに、ISO 27001 や FedRAMP℠ など、AWS がサポートするその他の認証では、ベストプラクティスの物理統制や環境統制が必要です。
クライアント側の保護	AWS 環境では PC や携帯機器などのクライアントからのアクセスをユーザーが保護および管理できますか?	はい。AWS では、お客様の要件に合わせて、お客様がクライアントおよびモバイルアプリケーションを管理できます。
サーバーのセキュリティ	ユーザーによる仮想サーバーの保護を許可していますか?	はい。AWS では、お客様独自のセキュリティアーキテクチャを実装できます。サーバーおよびネットワークのセキュリティの詳細については、AWS セキュリティホワイトペーパーをご覧ください。

カテゴリ	クラウドコンピューティングに関する質問	AWS の情報
アイデンティティ管理とアクセス管理	サービスに IAM 機能は含まれますか?	AWS には Identity and Access Management (IAM) サービスシリーズがあるため、お客様は、ユーザー ID の管理、セキュリティ認証情報の割り当て、ユーザーのグループ化による整理、ユーザーのアクセス許可の管理を一元的に行うことができます。詳細については、AWS ウェブサイトをご覧ください。
保守による停止の予定	保守目的でシステムを停止する予定が決められていますか?	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はありません。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。インスタンス自体の保守はお客様が統制します。
拡張機能	ユーザーが元々の契約を超えて拡張することを許可していますか?	AWS クラウドは分散され、セキュリティと復元力が高く、大きな拡張性のポテンシャルがあります。お客様は、利用した分の料金のみを支払う形で、拡張または縮小できます。
サービスの可用性	高レベルの可用性を確約していますか?	AWS は、サービスレベルアグリーメント (SLA) で高レベルの可用性を確約しています。例えば、Amazon EC2 は、1 年のサービス期間で 99.95% 以上の稼働時間を確約しています。Amazon S3 は毎月 99.9% 以上の稼働時間を確約しています。こうした可用性の評価指標が基準に満たない場合は、サービスクレジットが提供されます。
分散型サービス妨害 (DDoS) 攻撃	DDoS 攻撃に対してサービスをどのように保護していますか?	AWS ネットワークは、既存のネットワークセキュリティの問題に対する強固な保護機能を備えており、お客様はさらに堅牢な保護を実装することができます。DDoS 攻撃の説明などの詳細については、関連する AWS のセキュリティホワイトペーパーをご覧ください。

カテゴリ	クラウドコンピューティングに関する質問	AWS の情報
データの可搬性	AWS 環境に保存されているデータは、ユーザーが依頼すればエクスポートできますか?	AWS では、お客様の必要に応じて AWS ストレージへのデータの入出力が許可されています。S3 用 AWS Import/Export サービスでは、転送用のポータブル記憶装置を使用して、AWS 内外への大容量データの転送を高速化できます
サービスプロバイダーのビジネス継続性	ビジネス継続性プログラムを運用していますか?	AWS では、ビジネス継続性プログラムを運用しています。詳細な情報については、AWS セキュリティホワイトペーパーをご覧ください。
ユーザーのビジネス継続性	ユーザーがビジネス継続性計画を実装することは可能ですか?	AWS では、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。例えば、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。
データの耐久性	サービスでは、データの耐久性を規定していますか?	Amazon S3 は極めて堅牢性の高いストレージインフラストラクチャを提供しています。オブジェクトは冗長化のため、同一の Amazon S3 リージョン内の複数施設に分散した複数のデバイスに保存されます。一旦格納されると、Amazon S3 は冗長性が失われた場合にすばやく検出して修復することによってオブジェクトの堅牢性を維持します。Amazon S3 は、チェックサムを用いて、格納されているデータの完全性を定期的に検証しています。破損が検出されると、冗長データを使用して修復されます。S3 に保存されるデータは、1 年間にオブジェクトに対して 99.999999999% の堅牢性と 99.9% の可用性を提供するよう設計されています。

カテゴリ	クラウドコンピューティングに関する質問	AWS の情報
バックアップ	テープへのバックアップサービスは提供されていますか?	AWS では、お客様がご自分のテープバックアップサービスプロバイダを使用してテープへのバックアップを実行することが可能です。ただし、AWS ではテープへのバックアップサービスを提供していません。Amazon S3 サービスはデータ損失の可能性をほぼ 0% にまで低減する設計になっており、データストレージの冗長化によってデータオブジェクトのマルチサイトコピーに匹敵する永続性を実現しています。データの永続性と冗長性については、AWS のウェブサイトをご覧ください。
値上げ	突然値上げを行うことがありますか?	AWS にはサービス提供のコストが徐々に下がるにつれて、料金を頻繁に下げてきた歴史があります。AWS はここ数年間でも継続的に値下げを行っています。
サステナビリティ	AWS には長期間のサステナビリティがありますか?	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 には、非常に長期間のサステナビリティがあります。

詳細情報

詳細については、以下のソースを参照してください。

- AWS リスクとコンプライアンスの概要
- AWS の認定、プログラム、レポート、およびサードパーティーによる証明
- CSA Consensus Assessments Initiative Questionnaire

ドキュメントの改訂

変更	説明
2017 年 9 月	日本語版発行
2017 年 1 月	新しいテンプレートに移行しました。
2016 年 1 月	英語初版発行