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

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

AWS は外部の認定機関および独立監査人と協力し、AWS が制定、運用するポリシー、プロセス、統制に関する重要な情報をお客様に提供しています。

CJIS

AWS は FBI の Criminal Justice Information Services (CJIS) の基準に準拠しています。また、CJIS セキュリティポリシーに沿って従業員の必要な身元調査を許可および実行するなどの内容を盛り込んだ、CJIS セキュリティ契約をお客様と締結しています。

法執行機関のお客様 (および Criminal Justice Informaiton, CJI を管理するパートナー様) も AWS の高度なセキュリティサービスおよび AWS の関連する特性を活用して CJI データのセキュリティと保護を向上させています。これらのサービスには、アクティビティロギング (AWS CloudTrail)、移送中または保存中のデータの暗号化 (独自のキーを使用するオプションを含めた S3 のサーバー側の暗号化)、総合的なキー管理および保護 (AWS Key Management Service および CloudHSM)、統合されたアクセス権管理 (IAM フェデレーティッド認証管理、Multi-Factor Authentication) 等が含まれます。

AWS では、CJIS ポリシー対象範囲に合わせたセキュリティ計画テンプレートにより、Criminal Justice Information Services (CJIS) ワークブックを作成しています。さらに、CJIS ホワイトペーパーは、クラウド導入段階の顧客を支援するために開発されました。

CJIS Hub のページ (https://aws.amazon.com/compliance/cjis/) にアクセスしてください。

CSA

2011 年にクラウドセキュリティアライアンス (CSA) はクラウドプロバイダー間でセキュリティ慣行の透明性を推進するための STAR イニシアチブを立ち上げました。CSA セキュリティ、信頼性、保証の登録 (STAR) は無料の一般アクセス可能な登録で、さまざまなクラウドコンピューティングサービスが提供するセキュリティコントロールが文書化されており、ユーザーが現在使用中または契約を検討中のクラウドプロバイダーのセキュリティを評価するのに役立ちます。AWS は CSA STAR に登録しており、クラウドセキュリティアライアンス (CSA) の「Consensus Assessments Initiative Questionnaire (CAIQ)」に回答済みです。CSA が発行するこの CAIQ は、どのようなセキュリティ統制が AWS の IaaS (サービスとしてのインフラストラクチャ) 内に存在するかを参照し、文書化する手段の 1 つとなっています。CAIQ には、クラウド使用者およびクラウド監査人がクラウドプロバイダーに尋ねる可能性がある 298 個の質問が記載されています。

CSA Consensus Assessments Initiative Questionnaire を参照してください。

Cyber Essentials Plus

Cyber Essentials Plus は、英国政府の支援により業界がサポートする英国発の認定スキーマで、組織が一般的なサイバー攻撃に対して運用上のセキュリティを実証するのに役立ちます。

この認定は、英国政府が提供する「10 Steps to Cyber Security (サイバーセキュリティへの 10 ステップ)」のコンテキスト内で、一般的なインターネットベースの脅威がもたらすリスクを緩和するために AWS が実装しているベースラインコントロールを示しています。この認定は Federation of Small Businesses、Confederation of British Industry、保険会社などを含む多くの企業・業界団体が支援しており、取得した事業体にインセンティブを提供しています。

Cyber Essentials では必要とされるテクニカル・コントロールが規定されています。関連する保証フレームワークでは、認定評価機関が毎年行う外部評価を通じて Cyber Essentials Plus 認定での独立した保証プロセスがどのように機能するかが明らかになっています。認定は地域特性が高いため、欧州 (アイルランド) リージョンに限定されています。

DoD SRG レベル 2 および 4

国防総省 (DoD) クラウドセキュリティモデル (SRG)で は、クラウドサービスプロバイダ —(CSPs) が DoD プロビジョナル認証を取得するための正式な評価と許可のためのプロセスが提供されており、 DoD のお客様にこれを活用していただくことが可能です。SRG のプロビジョナル認証では、AWS が DoD の基準に準拠していることを証明する繰り返し利用可能な認定が発行され、DoD ミッション所有者が該当するシステムを AWS で運用するための評価および認可に必要な時間が削減できます。AWS では現在、SRG レベル 2 および 4 でプロビジョナル認証を取得しています。

セキュリティコントロールベースラインで定義されているレベル 2、4、5、6 の詳細情報については、次を参照してください。
http://iase.disa.mil/cloud_security/Pages/index.aspx

また、DoD Hub のページ (https://aws.amazon.com/compliance/dod/) も合わせて参照してください。

FedRAMPsm

AWS は、Federal Risk and Authorization Management Program (FedRAMPsm) に準拠したクラウドサービスプロバイダです。AWS は認定された第三者評価組織 (3PAO) である FedRAMPsm によって実施されるテストを完了し、FedRAMPsm 要件に Moderate インパクト・レベルで準拠することを示して、米国保健福祉省 (HHS) により 2 つの Agency Authority to Operate (ATO) を取得ています。すべての米国政府機関は、FedRAMPsm レポジトリに保存されている AWS Agency ATO パッケージを利用して、アプリケーションやワークロードに対する AWS の評価、AWS の利用許可の付与、AWS 環境へのワークロードの移行を行うことができます。2 つの FedRAMPsm Agency ATO はすべての米国リージョン (AWS GovCloud (US) リージョンおよび AWS 米国東部/西部リージョン) に対応しています。

次のサービスは、上記のリージョンの認定範囲内に含まれます。

- **Amazon Redshift** — Amazon Redshift は、高速で完全マネージド型のペタバイト規模を誇るデータウェアハウスサービスです。シンプルかつ費用対効果に優れているため、お客様はすべてのデータを既存のビジネスインテリジェンスツールで効率的に分析できます。詳細については、こちらを参照してください。
- **Amazon Elastic Compute Cloud (Amazon EC2)** — Amazon EC2 では、クラウド内でサイズ変更可能なコンピューティング容量を提供しています。ウェブスケールの処理能力を開発者が簡単に利用できるよう設計されています。詳細については、こちらを参照してください。

- **Amazon Simple Storage Service (S3)** – Amazon S3 を利用すれば、シンプルなウェブサービスインターフェイスを使用して、いつでも、ウェブ上のどこからでも、容量に関係なくデータを保存および取得できます。詳細については、こちらを参照してください。
- **Amazon Virtual Private Cloud (VPC)** – Amazon VPC を利用して、AWS の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内で AWS リソースを起動できます。詳細については、こちらを参照してください。
- **Amazon Elastic Block Store (EBS)** – Amazon EBS のストレージボリュームは、予測可能で、可用性と信頼性に優れており、稼働中の Amazon EC2 インスタンスにアタッチしてそのインスタンス内で 1 つのデバイスとして公開できます。詳細については、こちらを参照してください。
- **AWS Identity and Access Management (IAM)** – IAM により、ユーザーの AWS のサービスとリソースへのアクセスを安全にコントロールできます。IAM を使用すると、AWS のユーザーとグループを作成および管理し、アクセス権を使用して AWS リソースへのアクセスを許可および拒否できます。詳細については、こちらを参照してください。

AWS FedRAMPsm への準拠の詳細については、AWS の FedRAMPsm に関するよくある質問 (https://aws.amazon.com/compliance/fedramp/) を参照してください。

FERPA

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C.§ 1232g; 34 CFR Part 99) は、学生の教育記録のプライバシーを保護する連邦法です。同法は、米教育省の該当するプログラムで資金援助を受けているすべての学校に適用されます。FERPA では、子供の学校成績に関する特定の権利を親に委ねています。これらの権利は、子供が 18 歳になるか、子供が高校より上のレベルの学校に通うようになると、その子供に移行されます。権利が移行された学生は「有資格学生」となります。

AWS では、FERPA が適用される該当事業者およびビジネスアソシエイトに対して、保護された学生教育情報の処理、維持、および保管について安全な AWS 環境を提供しています。

AWS では、成績データの処理や保存に AWS の活用をお考えのお客様向けに、FERPA 関連のホワイトペーパーもご用意しています。

FERPA Compliance on AWS ホワイトペーパーは、コンプライアンスを促進するシステムを運用する方法の企業向け概要説明となっています。

FIPS 140-2

連邦情報処理規格 (Federal Information Processing Standard/FIPS) 出版物 140-2 は、機密情報を保護する暗号モジュールのセキュリティ要件を規定する米国政府のセキュリティ基準です。FIPS 140-2 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 (US) 内の SSL 終端装置は、FIPS 140-2 検証済みハードウェアを使用して運用されています。AWS では、AWS GovCloud (US) 環境をご利用いただくときのコンプライアンス管理に役立つ情報をお客様に提供しています。

FISMA と DIACAP

AWS 環境では、米国政府機関のシステムを連邦情報セキュリティマネージメント法 (Federal Information Security Management Act/FISMA) に準拠した状態で運用することができます。AWS インフラストラクチャは、該当するシステムの所有者の承認プロセスの一環として、多様な政府機関システムの独立査定人によって評価されています。多数の米国政府機関の勤務者と国防省 (DoD) が、NIST 800-37 および DoD Information Assurance Certification and Accreditation Process (DIACAP) に定義されているリスク管理フレームワーク (RMF) プロセスに従い、AWS クラウドでホストされているシステムのセキュリティ認可取得を達成しています。

GxP

GxP は、食品および薬、医療機器、医療ソフトウェアアプリケーションなどの医療製品を製造するライフサイエンス組織に適用される規制やガイドラインを指す略語です。GxP 要件では、食品や医療製品の消費者に対する安全性を確保し、製品に関連した安全性についての意思決定に使用されるデータの完全性を確保することが目的とされています。

AWS は、GxP ホワイトペーパーを公開し、GxP システム向けに AWS クラウドを使用するための包括的なアプローチの方法について詳しく紹介しています。このホワイトペーパーでは、GxP での AWS 製品の使用に関するガイダンスも示されています。このような内容については、検証済みの GxP システムで AWS の製品を現在使用中の製薬会社や医療機器メーカーのお客様、およびパートナーと共同で作成されました。

GxP のコンプライアンスに関連する詳細をリクエストするには、AWS 日本担当チームおよび事業開発にお問い合わせください。

日本において、AWS は AWS の GxP に関連するパートナー様と共同で日本の薬機法の規制内容に準拠する必要のあるお客様を、日本のガイドラインや商習慣に基づき、より良く支援していくための継続的な取り組みを行っています。

詳細は下記のページを参照ください。
https://aws.amazon.com/jp/compliance/gxp-part-11-annex-11/

HIPAA

米国医療保険の携行性と責任に関する法律 (HIPAA) の対象となる事業体とその取引先は、保護すべき医療情報を安全に処理、管理、保存できる環境として AWS 環境を利用しています。AWS はこのようなお客様と事業提携契約を結んでゆきたいと考えています。AWS では、医療情報の処理や保存に AWS の活用をお考えのお客様向けに、HIPAA 関連のホワイトペーパーもご用意しています。Architecting for HIPAA Security and Compliance on Amazon Web Services ホワイトペーパーは、AWS を利用して HIPAA と経済的および臨床的健全性のための医療 IT に関する法律 (HITECH) コンプライアンスを促進するシステムを運用する方法についての概要説明となっています。

お客様は、特定の HIPAA アカウントの下で任意の AWS のサービスを使用できますが、BAA で定義された HIPAA の対象サービスでのみ、PHI を処理、保存、転送可能です。現在、HIPAA の対象サービスは 9 つあります(2017, 1 月時点)。

- Amazon DynamoDB
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)

- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (Amazon RDS)、MySQL および Oracle エンジンのみを使用
- Amazon Simple Storage Service (S3)

AWS は標準ベースのリスク管理プログラムに従って、HIPAA の対象サービスが、HIPAA で要求されるセキュリティ、統制、管理の各プロセスをサポート可能なことを確認しています。これらのサービスを使用して PHI を保存、処理することで、お客様と AWS はユーティリティベースの運用モデルに該当する HIPAA 要件に対応することができます。AWS は、お客様の要求に応じて新しい対象サービスに優先順位を付けて追加しています。

詳細については、HIPAA コンプライアンスに関するよくある質問および Architecting for HIPAA Security and Compliance on Amazon Web Services を参照してください。

最新の対象サービスのリストについては、下記の URL を参照ください。
https://aws.amazon.com/compliance/services-inscope/

IRAP

Information Security Registered Assessors Program (IRAP) では、オーストラリア政府のお客様が適切なコントロールの導入について検証可能であり、Australian Signals Directorate (ASD) Information Security Manual (ISM) の必要に対応した適切な責任モデルを特定するのに役立ちます。

アマゾン ウェブ サービスでは独立した評価を完了しており、AWS シドニーリージョンの非機密情報 (DLM) の処理、ストレージ、および伝送において、該当するすべての ISM コントロールが導入されていることを確認しています。

詳細については、IRAP コンプライアンスに関するよくある質問 (https://aws.amazon.com/compliance/irap/) およびオーストラリア信号局 (ASD) のクラウドコンピューティングに関するセキュリティ上の考慮事項への AWS の準拠を参照してください。

ISO 9001

AWS は ISO 9001 認証を取得しており、AWS の ISO 9001 認証は AWS クラウドで品質管理された IT システムを開発、移行、運用するお客様を直接サポートするものです。お客様は、独自の ISO 9001 プログラムや業界別の品質プログラム (ライフサイエンスでの GxP、医療機器での ISO 13485、航空宇宙産業での AS9100、自動車産業での ISO/TS 16949 など) の認証取得に、AWS の ISO9001 認証レポートを活用できます。品質システムの要件がないお客様にも、ISO 9001 認証により AWS の保証や透明性が向上するというメリットがあります。

ISO 9001 認証は、AWS サービスと運用リージョン (下記) および次のサービスの指定された範囲の品質管理システムを対象としています。

- AWS CloudFormation
- AWS クラウドハードウェアセキュリティモデル (HSM)
- Amazon CloudFront
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- Amazon DynamoDB
- Amazon EC2 VM Import/Export
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)
- Amazon EC2 Container Service (ECS)
- Amazon Elastic File System (EFS)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache

- Amazon Glacier
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- AWS Storage Gateway
- Amazon Simple Workflow Service (SWF)
- Amazon Virtual Private Cloud (VPC)
- AWS WAF - ウェブアプリケーションファイアウォール
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- 基礎となる物理インフラストラクチャと AWS 管理環境

AWS の ISO 9001 認証が対象となる AWS リージョンには、米国東部 (バージニア北部)、米国西部 (オレゴン)、米国西部 (北カリフォルニア)、AWS GovCloud (米国)、南米 (サンパウロ)、欧州 (アイルランド)、欧州 (フランクフルト)、アジアパシフィック (シンガポール)、アジアパシフィック (シドニー)、およびアジアパシフィック (東京) が含まれます。

ISO 9001:2008 は製品とサービスの品質を管理するためのグローバルな規格です。9001 規格では、国際標準化機構 (ISO) の品質マネジメントおよび品質保証技術委員会が定義した 8 つの原則に基づいて、品質マネジメントシステムを概説しています。この 8 つの原則は以下のとおりです。

- 顧客重視
- リーダーシップ
- 人々の参画
- プロセスアプローチ
- マネジメントへのシステムアプローチ
- 継続的改善
- 意思決定への事実に基づくアプローチ
- 供給者との互恵関係

AWS ISO 9001 認証は、(https://do.awsstatic.com/certifications/iso_9001_certification.pdf) でダウンロードできます。AWS は、ISO 9001 認定に関する追加情報とよくある質問を次のウェブサイトで提供しています。https://aws.amazon.com/compliance/iso-9001-faqs/。

最新の対象サービスのリストについては、下記の URL を参照ください。https://aws.amazon.com/compliance/services-inscope/

ISO 27001

AWS は、AWS のインフラストラクチャ、データセンター、サービスを対象とした Information Security Management System (ISMS) に関連する ISO 27001 認証を達成しています。対象となるサービスは以下のようなものですが、最新の対象サービスのリストについては、下記の URL を参照ください。
https://aws.amazon.com/compliance/services-inscope/

- AWS CloudFormation
- Amazon CloudFront
- AWS Cloudtrail
- AWS Directory Service
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)
- Amazon EC2 Container Service (ECS)
- AWS Direct Connect
- Amazon EC2 VM Import/Export
- AWS クラウドハードウェアセキュリティモデル (HSM)
- Elastic Load Balancing (ELB)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- AWS Route 53

- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)
- AWS WAF - ウェブアプリケーションファイアウォール
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- 基礎となる物理インフラストラクチャ (GovCloud を含む) と AWS の統制環境

ISO 27001/27002 はグローバルに広く採用されているセキュリティ標準であり、事業と顧客情報の管理について、刻々と変化する脅威のシナリオに適する定期的リスク査定に基づいた、体系的なアプローチの要件とベストプラクティスが規定されています。認証を取得するためには、事業とカスタマー情報の機密性、完全性、および可用性に影響を与える情報セキュリティリスクを管理する体系的かつ継続的なアプローチが会社にあることを示す必要があります。この認証は、セキュリティに関連する統制や実践に関する重要情報をお客様に提供するという Amazon のコミットメントを強化するものです。

AWS の ISO 27001 認定が対象となる AWS リージョンには、米国東部 (バージニア北部)、米国西部 (オレゴン)、米国西部 (北カリフォルニア)、AWS GovCloud (米国)、南米 (サンパウロ)、欧州 (アイルランド)、欧州 (フランクフルト)、アジアパシフィック (シンガポール)、アジアパシフィック (シドニー)、およびアジアパシフィック (東京) が含まれます。

AWS ISO 27001 認証は、(https://do.awsstatic.com/certifications/iso_27001_global_certification.pdf) でダウンロードできます。

AWS は、ISO 27001 認定に関する追加情報とよくある質問を次のウェブサイトで提供しています。https://aws.amazon.com/compliance/iso-27001-faqs/。

ISO 27017

ISO 27017 は国際標準化機構 (ISO) が発行する新しい実践のための規範です。特にクラウドサービスに関係した情報セキュリティ統制の実装におけるガイダンスを提供しています。

AWS は、次のものを含む 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 27017 認定を達成しています。対象となるサービスは以下のようなものですが、最新の対象サービスのリストについては、下記の URL を参照ください。https://aws.amazon.com/compliance/services-inscope/

- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2 Container Service (ECS)
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (RDS)

- Amazon Route 53
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- AWS Storage Gateway
- AWS WAF (ウェブアプリケーションファイアウォール)
- Elastic Load Balancing
- VM Import/Export

AWS ISO 27017 認証は、(https://do.awsstatic.com/certifications/iso_27017_certification.pdf) からダウンロードできます。

AWS では、ISO 27017 認定に関する追加情報とよくある質問を (https://aws.amazon.com/compliance/iso-27017-faqs/) で提供しています。

ISO 27018

ISO 27018 は、クラウドにおける個人データの保護に焦点を当てた最初の国際的な実践のための規範です。ISO 情報セキュリティ規格 27002 に基づいており、パブリッククラウドの個人識別情報 (Personal Identifiable Informaiton , PII) に適用される ISO 27002 統制の実装ガイダンスを提供しています。また、既存の ISO 27002 コントロールセットでは対応していないパブリッククラウド PII 保護要件に対応するための追加のコントロールセット、および関連ガイダンスも提供しています。

AWS は、次のものを含む 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) における ISO 27018 認定を達成しています。対象となるサービスは以下のようなものですが、最新の対象サービスのリストについては、下記の URL を参照ください。https://aws.amazon.com/jp/compliance/services-inscope/

- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2 Container Service (ECS)
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (RDS)

- Amazon Route 53
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- AWS Storage Gateway
- AWS WAF (ウェブアプリケーションファイアウォール)
- Elastic Load Balancing
- VM Import/Export

AWS ISO 27018 認証は、(https://do.awsstatic.com/certifications/iso_27018_certification.pdf) でダウンロードできます。

AWS では、ISO 27018 認定に関する追加情報とよくある質問を (https://aws.amazon.com/compliance/iso-27018-faqs/) で提供しています。

ITAR

AWS GovCloud (US) リージョンでは、武器規制国際交渉規則 (ITAR) コンプライアンスをサポートしています。包括的な ITAR コンプライアンスプログラム管理の一環として、ITAR 輸出規制の対象となる企業は、保護されたデータへのアクセスを米国人に制限し、およびそのデータの物理的なロケーションを米国の土地に制限することによって、意図しない輸出を制御する必要があります。AWS GovCloud（米国）は、物理的に米国に位置し、そこでは AWS のスタッフによるアクセスを米国人に制限するという環境を提供しているため、適格企業は、ITAR の規制対象となる、保護された文書およびデータを送信、処理、格納することができます。AWS GovCloud（米国）環境は、この要件において、顧客の輸出コンプライアンスプログラムをサポートする適切な統制がなされているかどうかを検証するために、独立したサードパーティーによる監査を受けています。

MPAA

アメリカ映画協会 (MPAA) は、保護されたメディアとコンテンツを安全に保存、処理、配給するための一連のベストプラクティスをまとめました (http://www.fightfilmtheft.org/facility-security-program.html)。メディア企業ではこのベストプラクティスを、コンテンツとインフラストラクチャのリスクとセキュリティを評価する手段として使用しています。AWS は MPAA のベストプラクティスに準拠していることが実証されており、AWS のインフラストラクチャはすべての適用可能な MPAA インフラストラクチャコントロールに準拠しています。MPAA は「証明書」を提供していませんが、メディア業界のお客様は AWS の MPAA 型コンテンツのリスク査定および評価を補足する AWS MPAA 文書を使用することができます。

AWS Compliance MPAA 保証プログラムの詳細は、(https://www.aws.amazon.com/compliance/mpaa/) をご覧ください。

MTCS Tier 3 認定

Multi-Tier Cloud Security（MTCS）は、シンガポールで運用されているセキュリティ管理規格（SPRING SS 584:2013）で、ISO 27001/02 Information Security Management System（ISMS）規格に基づいています。この認証審査では次を行う必要があります。

- 情報セキュリティリスクを体系的に評価し、企業の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制御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
- 包括的な管理プロセスを採用し、継続的に情報セキュリティ制御が情報セキュリティのニーズを満たすようにする

MTCS Hub ページ (https://aws.amazon.com/jp/compliance/aws-multitiered-cloud-security-standard-certification/) をご覧ください。

NIST

2015 年 6 月に、米国標準技術局 (NIST) はガイドライン 800-171、"Final Guidelines for Protecting Sensitive Government Information Held by Contractors" を発表しました。このガイダンスは、連邦システム以外の管理指定された非機密扱いの情報 (Controlled Unclassified Information/CUI) に適用されます。

AWS は既にこれらのガイドラインに準拠しており、お客様は実質的にすぐにでも NIST 800-171 に準拠することができます。NIST 800-171 では、NIST 800-53 要件のサブセットについて説明しています。このガイドラインに基づいて、AWS はすでに FedRAMP プログラムで監査を受けています。FedRAMP Moderate セキュリティ・コントロール・ベースラインは 800-171 の第 3 章で言及されている推奨要件よりも厳格で、CUI データを保護する FISMA Moderate システムの要求を上回るセキュリティコントロールが数多く含まれています。詳細なマッピングについては、NIST Special Publication 800-171 の D2 ページ (PDF 版では 37 ページ) を参照してください。

PCI DSS レベル 1

AWS は、Payment Card Industry (PCI) データセキュリティ基準 (Data Security Standard/DSS) のレベル 1 に準拠しています。お客様は、PCI 準拠のテクノロジーインフラストラクチャである AWS 環境上において、クレジットカード情報を保管、処理、送信するアプリケーションを実行することができます。2013 年 2 月、PCI Security Standards Council は、PCI DSS Cloud Computing Guidelines をリリースしました。このガイドラインでは、カード保有者のデータ環境を管理しているお客様向けに、AWS 環境上での PCI DSS 管理作業の留意事項を記載し提供しています。AWS では、お客様向けに PCI DSS Cloud Computing Guidelines を AWS PCI Compliance Package に組み込んでいます。AWS PCI Compliance Package には、AWS PCI Attestation of Compliance (AoC) と AWS PCI Responsibility Summary が含まれています。前者では、AWS が PCI DSS Version 3.1 においてレベル 1 サービス プロバイダに適用される標準を満たしていることが検証されています。後者では、AWS とお客様の間でコンプライアンスに関する責任をどのように分担するかが説明されています。

PCI DSS レベル 1 の対象となるサービスは以下のようなものですが、最新の対象サービスのリストについては、下記の URL を参照ください。
https://aws.amazon.com/jp/compliance/services-inscope/

- Auto Scaling
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- AWS Key Management Service (KMS)
- AWS Identity and Access Management (IAM)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon SimpleDB
- Amazon Simple Storage Service (S3)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Workflow Service SWF
- Amazon Virtual Private Cloud (VPC)

- 基礎となる物理インフラストラクチャ (GovCloud を含む) と AWS 管理環境

AWS PCI DSS レベル 1 認証のサービスの最新の範囲は、「PCI DSS レベル 1 に関するよくある質問」 (https://aws.amazon.com/compliance/pci-dss-level-1-faqs/) に記載されています。

SOC 1/ISAE 3402

アマゾン ウェブ サービスは Service Organization Controls 1 (SOC 1)、Type II レポートを発行しています。このレポートの監査は、米国公認会計士協会 (AICPA)AT 801 (旧称 SSAE 16) および International Standards for Assurance Engagements 第 3402 号 (ISAE 3402) に従って実施されます。この 2 つの基準によるレポートは、米国および国際的な会計監査機関の監査における幅広い要件を満たすために作成されています。SOC 1 レポートの監査は、AWS の統制目標が適切に設計されていること、およびカスタマーデータを保護するために定義された個々の統制が機能していることの有効性を証明するものです。このレポートは、従来の監査基準書第 70 号（SAS 70）Type II 監査レポートに代わるものです。

レポートには AWS SOC 1 の統制目標が記載されており、このレポート自体に、各統制目標と独立監査人による各統制のテスト手順の結果をサポートする統制活動が特定されています。

目標範囲	目標内容
セキュリティ組織	情報セキュリティポリシーが組織全体で実施され、伝達されていることについて、合理的な保証を提供するものです。

目標範囲	目標内容
従業員ユーザーによるアクセス	Amazon 従業員ユーザーアカウントが適時に追加、変更、および削除され、定期的にレビューされるように手順が確立されていることについて、合理的な確証を提供するものです。
論理的セキュリティ	データに対する許可のない内部的および外部的アクセスを適切に制限するためのポリシーとメカニズムが用意され、顧客データが他の顧客から適切に隔離されることについて、合理的な確証を提供するものです。
安全なデータ処理	AWS ストレージとお客様のデータ転送開始点の間のデータ処理がセキュリティで保護され、適切にマッピングされることについて、合理的な保証を提供するものです。
物理的なセキュリティと環境の予防手段	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にのみ制限し、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。
変更管理	既存の IT リソースに対する変更（緊急/特殊な設定）が記録され、認証され、試験され、承認されて文書化されることについて、合理的な保証を提供するものです。
データの完全性、可用性および冗長性	伝送、保管、処理など、すべての段階を通じてデータの完全性が維持されることについて、合理的な保証を提供するものです。
インシデント処理	統制は、システム障害が記録、分析、および解決されることについて、合理的な保証を提供するものです。

SOC 1 レポートは、ユーザー組織の財務諸表の監査に関連する可能性が高い、サービス組織の統制を中心に設計されています。AWS のお客様層は広く、AWS サービスの利用形態も同様に様々であるため、お客様の財務諸表に対する統制の適用可能性も、お客様ごとに異なります。そのため、AWS SOC 1 レポートは、会計監査時に必要になる可能性が高い、特定の主要な統制と、多様な使用方法と監査シナリオに合うために、幅広い IT の一般的な統制を対象に設計されています。そのため、お客様は会計のレポートプロセスに欠かせないデータなど、AWS インフラストラクチャを利用し、重要なデータを保存および処理可能です。AWS は、お客様からのフィードバック、およびこの重要な監査レポートの利用形態について考慮し、これらの統制の選択内容について定期的に再評価しています。

SOC 1 レポートに関する AWS の取り組みは継続中で、定期監査のプロセスを継続していく予定です。SOC1 レポートの対象は次のとおりですが、最新の対象サービスのリストについては、下記の URL を参照ください。
https://aws.amazon.com/jp/compliance/services-inscope/

- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2 VM Import/Export
- Amazon Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon ElastiCache
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Load Balancing (ELB)

- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow (SWF)
- Amazon Simple Queue Service (SQS)
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkSpaces

SOC 2

AWS では SOC 1 レポートに加え、Service Organization Controls 2 (SOC 2)、Type II レポートも発行しています。統制の評価という観点では SOC 1 と同様となりますが、 SOC 2 レポートでは米国公認会計士協会 (AICPA) の信用提供の原則 (Trust Services Principles) で定められている内容についても統制の評価に含まれた監査レポートになります。これらの原則では、AWS などのサービス組織に適用されるセキュリティ、可用性、処理の完全性、機密性、およびプライバシーに関連する実務的な統制が定義されています。AWS SOC 2 レポートは、そのような統制に関する設計と運用の有効性が、米国公認会計士協会 (AICPA) の信用提供の原則 (Trust Services Principles) で示されているセキュリティと可用性の原則の基準を満たしているかを評価した内容となっています。このレポートは、最新の実践として事前定義された標準に基づいて AWS のセキュリティと可用性に関し

て一層の透明性を与え、AWS の顧客データ保護に対する取り組みを明らかにするものです。SOC 2 レポートの範囲には、SOC 1 レポートの対象と同じサービスが含まれます。対象となるサービスの詳細については上記の SOC 1 の説明を参照してください。

SOC 3

AWS は Service Organization Controls 3（SOC 3）レポートを発行しています。SOC 3 レポートは、AWS SOC 2 レポートを一般公開用に要約したものです。レポートには、(SOC 2 レポートに含まれる AICPA の Security Trust Principles に基づく) 管理の操作の外部監査人の意見、制御の有効性に関する AWS マネジメントからの表明、AWS インフラストラクチャおよびサービスの概要が含まれます。AWS SOC 3 レポートには、対象サービスをサポートする世界中の AWS データセンターも全て含まれます。AWS SOC3 レポートは、 SOC 2 レポートを請求する手続きを踏まなくとも、AWS が外部監査人の保証を得ていることについて、簡易に確認できる便利な資料となっています。SOC 3 レポートの範囲には、SOC 1 レポートの対象と同じサービスが含まれます。対象となるサービスの詳細については上記の SOC 1 の説明を参照してください。AWS SOC 3 レポートは、こちらからご覧ください。

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
- 主要なコンプライアンスに関する質問と AWS の回答
- 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