



[AWS Black Belt Online Seminar]

AWS Audit Manager

サービスカットシリーズ



Security Solutions Architect
高橋 悟史
2021年3月9日

AWS 公式 Webinar
<https://amzn.to/JPWebinar>



過去資料
<https://amzn.to/JPArchive>



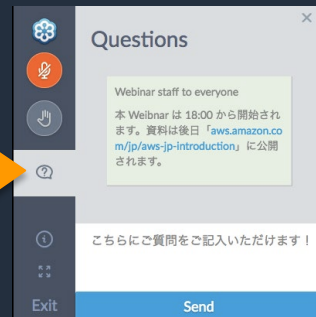
AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分かれて、アマゾンウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。

質問を投げることができます！

- 書き込んだ質問は、主催者にしか見えません
- 今後のロードマップに関するご質問はお答えできませんのでご了承下さい

- ① 吹き出しをクリック
- ② 質問を入力
- ③ Sendをクリック



Twitter ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- 本資料では2021年3月9日現在のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(<http://aws.amazon.com>)にてご確認ください。
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。
- 価格は税抜表記となっております。日本居住者のお客様には別途消費税をご請求させていただきます。
- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at <http://aws.amazon.com/agreement/>. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

自己紹介

高橋 悟史

アマゾン ウェブ サービス ジャパン 株式会社
シニア セキュリティ ソリューション アーキテクト
CISSP, CISM

経歴：IBM, McAfee, Salesforce.comを経て
2019年より AWS Japan でセキュリティ ソリューション アーキテクト
を担当

AWS をご利用のお客様に対するセキュリティに関する支援を担当



本日本話する内容

- 監査の目的と監査の種類
- AWS Audit Manager 概要
- AWS Audit Manager 構成要素
- AWS Audit Manager アーキテクチャパターン
- 設定方法、設定例
- セキュリティ、料金、制約
- パートナー様との協業
- まとめ

監査の目的と監査の種類

AWS Audit Manager 概要

AWS Audit Manager 構成要素

AWS Audit Manager アーキテクチャパターン

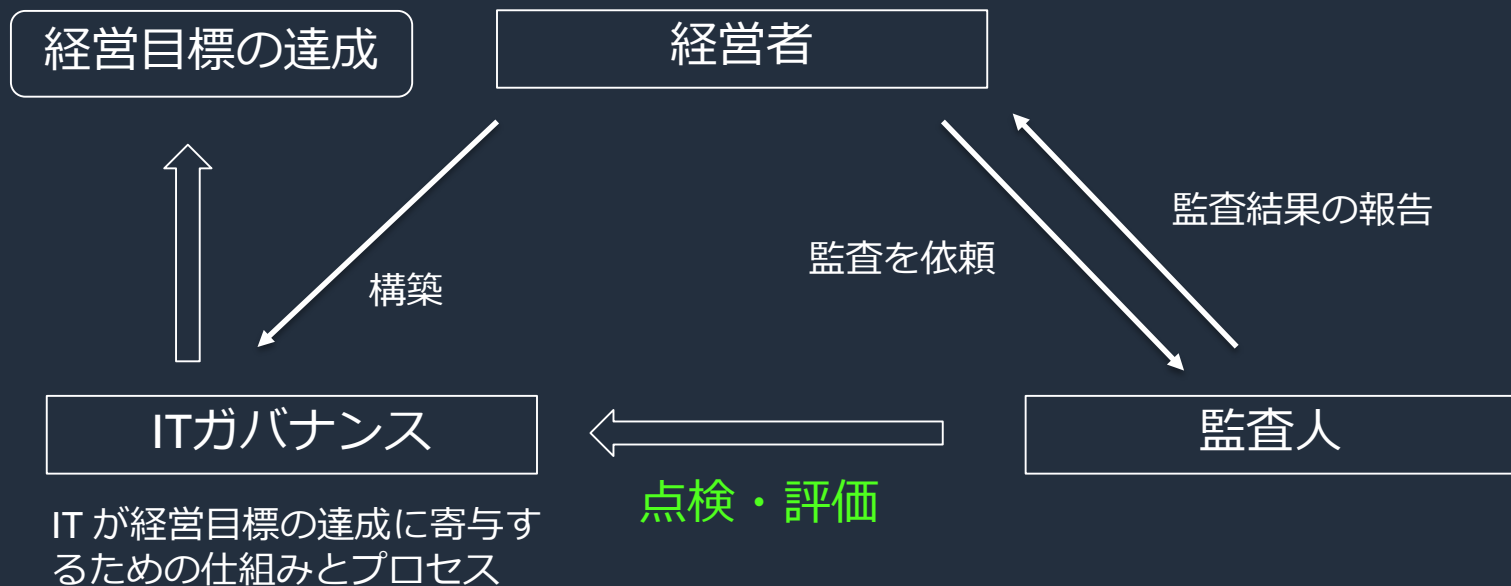
設定方法、設定例

セキュリティ、料金、制約

パートナー様との協業

まとめ

IT 監査/システム監査とは



個人情報保護法の施行や、金融商品取引法による内部統制報告、監査が必要になったことを背景に、経営者に代わって監査人がITガバナンスの点検、評価をして経営者に提言を行い改善をすることが必要になった

監査の種類

いくつかの観点で監査を分類することが出来る

監査形態	保証型監査	一定の基準を満たしているかについて監査人が保証意見を提示する監査（会計監査、SOC 監査）
	助言型監査	問題点を検出し、改善を提言する監査
監査主体	内部監査	組織内の内部統制の一貫として行われる監査
	外部監査	組織とは利害関係のない外部の専門家によって行われる、一定規模の企業や業種で義務付けられている
監査目的	システム監査	システム全体に対する監査。経済産業省が作成したシステム監査基準が存在する
	セキュリティ監査	情報セキュリティを対象とした監査。ISO 27001, 27002 のようなベストプラクティスがある
	認証取得のための監査	PCI DSS, ISMS, FedRAMP などの認定取得のための監査
	内部統制監査	企業の財務統制を評価する監査（J-SOX 監査等）

コンプライアンス標準と監査の例

コンプライアンス基準	監査の目的	管轄組織	監査対象	一時点監査 or 運用監査？	監査人
SOC (Systems and Organization Controls)	SOC1：財務報告に影響する内部統制の評価 SOC2：システムの有効性の評価	AICPA (米国公認会計士協会)	ポリシー、プロセス、組織、体制、システム実装、システム運用	Type1 (一時点の監査), Type 2 (半年以上の運用状況監査)	第三者監査法人 (資格 CPA が必要)
PCI DSS	クレジットカード情報の安全な取り扱い	PCI Security Standards Council	クレジットカード情報を取り扱うシステム	一時点	第三者監査法人 (資格 QSA が必要)
ISO/IEC 27001 (日本ではISMS)	情報セキュリティマネジメントシステムが構築され、適切に管理しているかを確認	ISO/IEC 日本工業標準調査会	情報システムに関わるマネジメントシステム	一時点	第三者監査法人 (資格が必要、ISMSでは審査員)
FedRAMP	米国政府期間が利用するクラウドサービスのセキュリティ認証	米国政府	米国政府期間が利用するクラウドサービス・プロバイダー	運用監査あり	認定された第三者機関
ISMAP	政府利用のための安全なクラウドサービス・プロバイダ認定	ISMAP運営委員会, IPA	日本政府、自治体が利用するクラウドサービス・プロバイダー	初年度は一時点、2年目以降は運用監査あり	ISMAP 運営委員会が認定した監査法人

※参考情報として調査した情報であり、詳細については、各標準や認定団体のWebサイトや資料を参照してください

監査の目的と監査の種類

AWS Audit Manager 概要

AWS Audit Manager 構成要素

AWS Audit Manager アーキテクチャパターン

設定方法、設定例

セキュリティ、料金、制約

パートナー様との協業

まとめ

AWS Audit Manager 概要

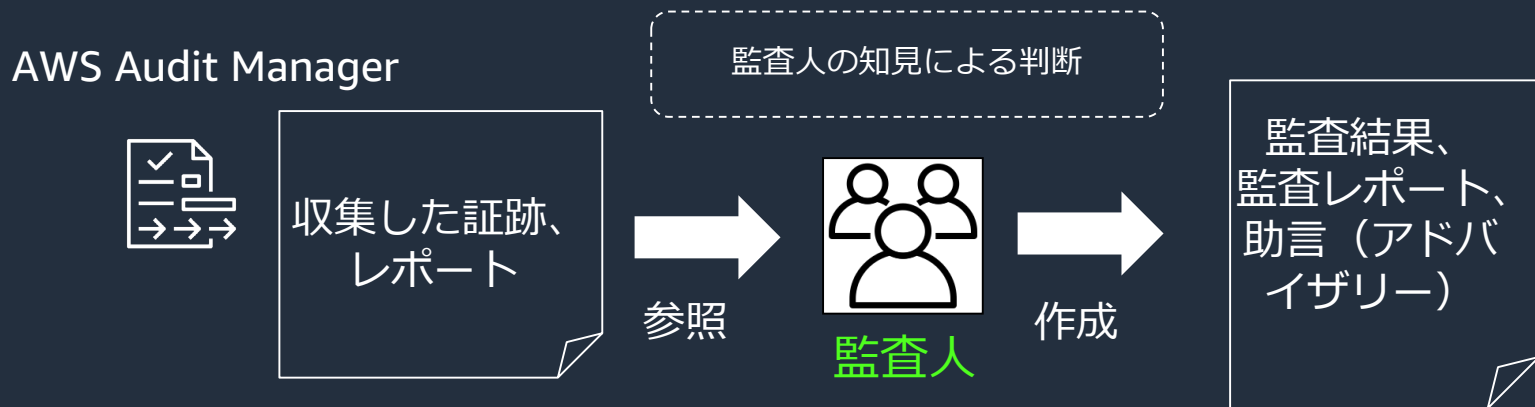
- AWS の使用状況を継続的に監査して、従来手動で行われていた証跡収集作業を削減し、AWSのプラットフォーム自体と同じくスケールする監査をサポートする
- AWS Audit Manager には CIS AWS Foundation Benchmark, GDPR, PCI DSS などの業界標準や認証が監査に要求する項目に対応するテンプレートが入っており、AWS 上の監査証跡を自動で収集します

- お客様にとってのメリット
 - 監査証跡の収集を手動で行う手間の削減

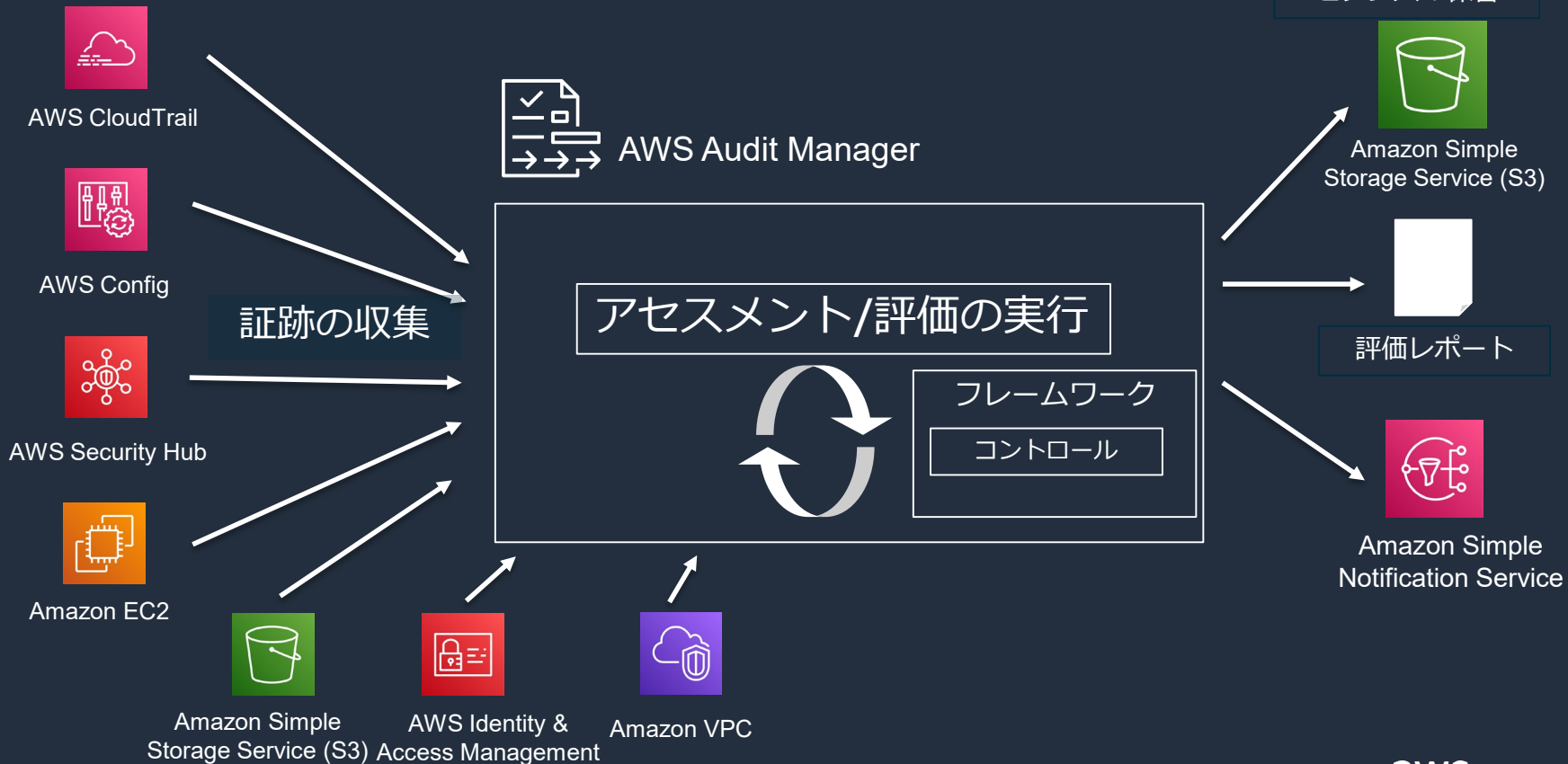
- 監査人が得るメリット
 - 監査証跡の収集を手動で行う手間の削減
 - 監査証跡の真正性が Audit Manager で担保される
 - リアルタイムに近い形で最新の証跡を取得出来る

AWS Audit Manager の監査における役割

- Audit Manager は監査業務そのものを代行するサービスではない
- Audit Manager は、内部監査や外部監査における証跡（エビデンス）収集を自動化し、監査人による監査の手間を削減するためのサービス



AWS Audit Manager アーキテクチャ



監査の目的と監査の種類

AWS Audit Manager 概要

AWS Audit Manager 構成要素

AWS Audit Manager アーキテクチャパターン

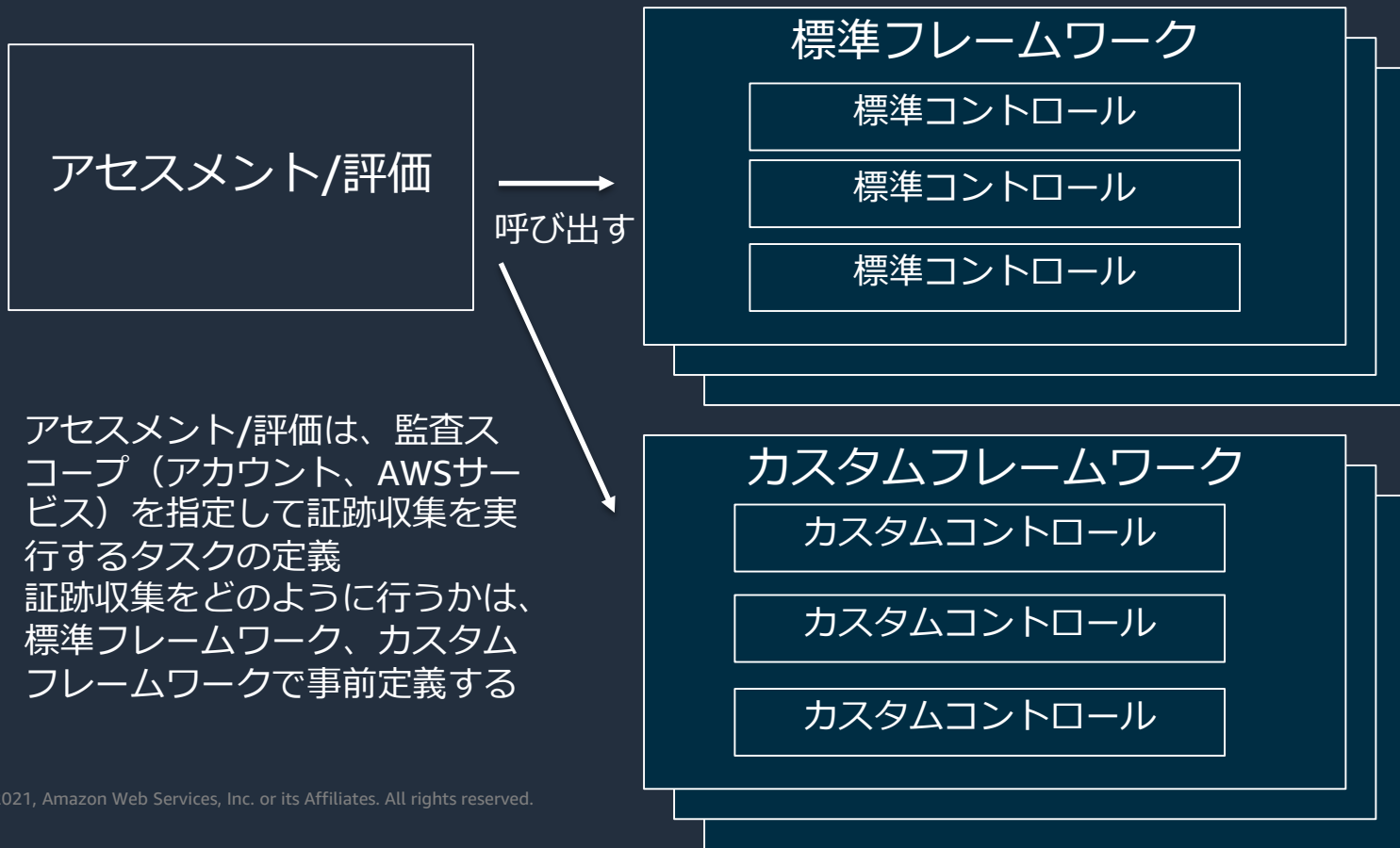
設定方法、設定例

セキュリティ、料金、制約

パートナー様との協業

まとめ

AWS Audit Manager 構成要素



Audit Manager が提供するフレームワーク 1

名称	説明	含まれる自動コントロールの数
AWS Audit Manager サンプルフレームワーク	検証用などでサンプルとして実行出来るフレームワーク	4
AWS Control Tower ガードレール	AWS Control Tower ガードレールで定義されているガイダンスを監査する	14
AWS License Manager	Microsoft, SAP, Oracle, IBMなどのソフトウェアベンダーのソフトウェア・ライセンスを監査する	27
AWS 運用のベストプラクティス (OBP)	AWS のベストプラクティスに基づいた監査項目	52
CIS Amazon Web Services Foundations Benchmark v1.2.0, レベル1および2用のCISベンチマーク	Center of Internet Security が提唱するAWS環境の基本的なチェック項目を監査する	45
CIS コントロール v7.1 実装グループ 1	Center of Internet Security が提唱する一般的な攻撃を緩和するためのベストプラクティスを監査する	21

参考 https://docs.aws.amazon.com/ja_jp/audit-manager/latest/userguide/framework-overviews.html

Audit Manager が提供するフレームワーク 2

名称	説明	含まれる自動コントロールの数
FedRAMP Allgress による中程度のベースライン	米国政府が展開しているクラウドサービス・プロバイダーのセキュリティ評価のチェック項目を監査する	376
GDPR	EU/EEAの個人情報保護に関するレギュレーションのチェック項目	0 (手動コントロールは376)
GxP 21 CFR part 11	消費者に対して食料と医薬品の安全を守るために生産時のデータ整合性を保証するレギュレーション	14
HIPAA	米国の個人健康保険情報を保護する連邦法で規定されている項目の監査	33
HITRUST v9.4 レベル 1	HIPAAを含む各種コンプライアンス標準を満たすためのフレームワーク	45
PCI DSS v3.2.1	クレジットカード業界のセキュリティ標準で定められているコントロールを監査する	152
SOC 2	米国公認会計士協会が定めているセキュリティや可用性に関する監査項目	35

フレームワークとコントロールの例

PCI DSS の例

コントロールセットとして、PCI DSS の要求事項の大項目がセクションとして並んでいて、セクションを展開すると個別の要求事項がコントロールとして含まれている

Controls grouped by control set	Type	Data source
▶ Requirement 1: Install and maintain a firewall configuration to protect cardholder data	-	-
▶ Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	-	-
▼ Requirement 3: Protect stored cardholder data	-	-
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	Standard	Manual
3.1.a Examine the data retention and disposal policies, procedures and processes to verify they include the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. • Specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons). • Processes for secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons. • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.	Standard	Manual
3.1.b Interview personnel to verify that: • All locations of stored cardholder data are included in the data retention and disposal processes. • Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data. • The quarterly automatic or manual process is performed for all locations of cardholder data.	Standard	Manual
3.1.c For a sample of system components that store cardholder data: • Examine files and system records to verify that the data stored does not exceed the requirements defined in the data retention policy • Observe the deletion mechanism to verify data is deleted securely.	Standard	AWS Config
3.2 Do not store sensitive authentication data (SAD) after authorization.	Standard	Manual
3.2.1 Do not store the expiration date, expiration time, or other sensitive information that identifies a session as valid after authorization.	Standard	AWS Config

自動コントロールと手動コントロール

AWS Audit Manager > Framework library > FedRAMP Moderate Baseline by Allgress

FedRAMP Moderate Baseline by Allgress (Read only)

Customize framework

Create assessment from framework

Framework details

Framework name

FedRAMP Moderate Baseline by Allgress

Compliance type

FedRAMP

Description

The Federal Risk and Authorization Management Program (FedRAMP) is a US government-wide program that provides Cloud Service Providers (CSPs) a standardized approach to security assessment, authorization, and continuous monitoring for their products and services and in doing so, provides assurance to federal agencies regarding the compliance of the CSPs controls related to their cloud offering.

Lists the moderate impact level controls within the FedRAMP Moderate Security Controls Baseline document for CSPs that will handle government data that is not publicly available by Allgress.

376 automated controls
835 manual controls

Framework type

Standard

Control sets

325

Controls

1211

Control sources

3

Tags

0

376個は自動コントロール。Audit Managerが自動的に証跡を収集する。
残る835個は手動コントロールなので、ユーザー側で証跡を Amazon S3 経由で Audit Managerにアップロードする必要がある

監査の目的と監査の種類

AWS Audit Manager 概要

AWS Audit Manager 構成要素

AWS Audit Manager アーキテクチャパターン

設定方法、設定例

セキュリティ、料金、制約

パートナー様との協業

まとめ

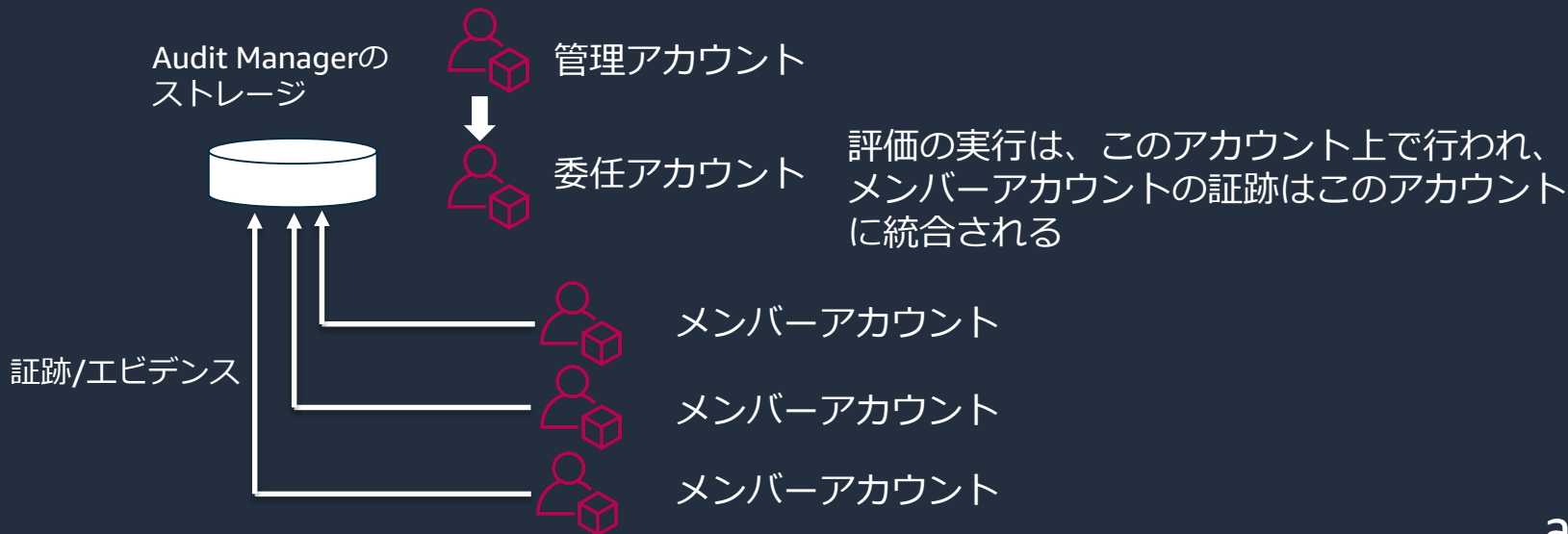
マルチアカウント環境の AWS Audit Manager

AWS Organizations 環境の場合、Audit Manager は評価を複数のアカウントで実行し、証跡/エビデンスを委任アカウントに統合することが可能

参照 : https://docs.aws.amazon.com/ja_jp/audit-manager/latest/userguide/setting-up.html#enabling-orgs

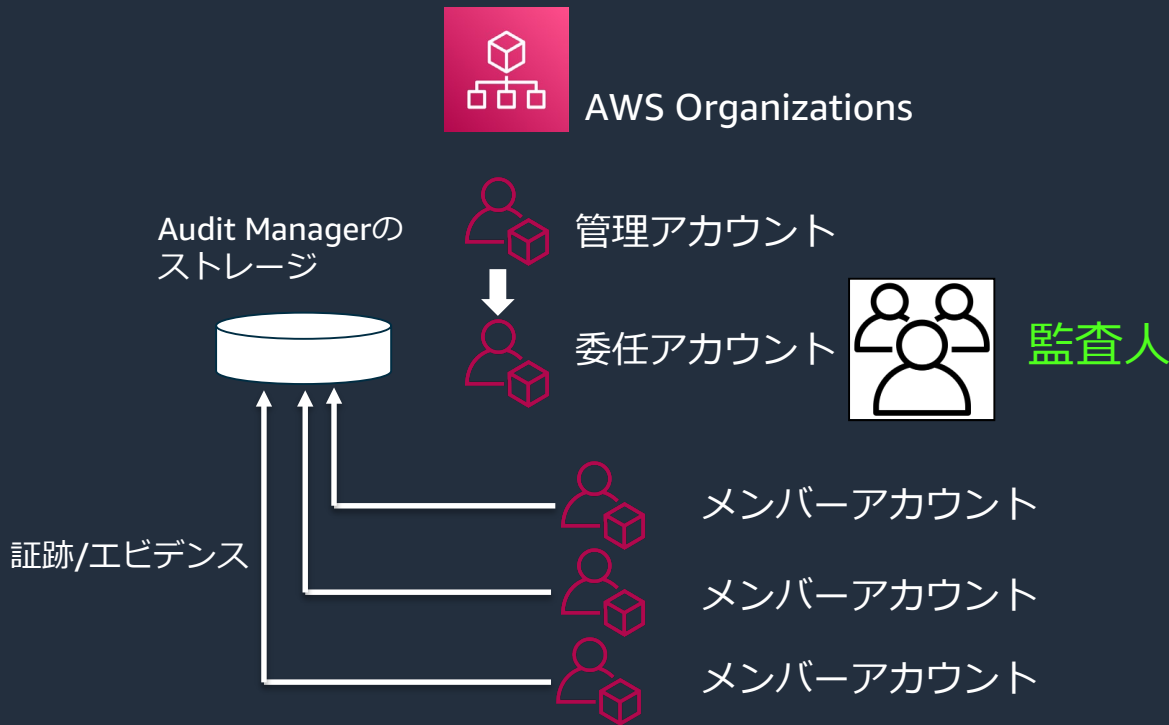


AWS Organizations



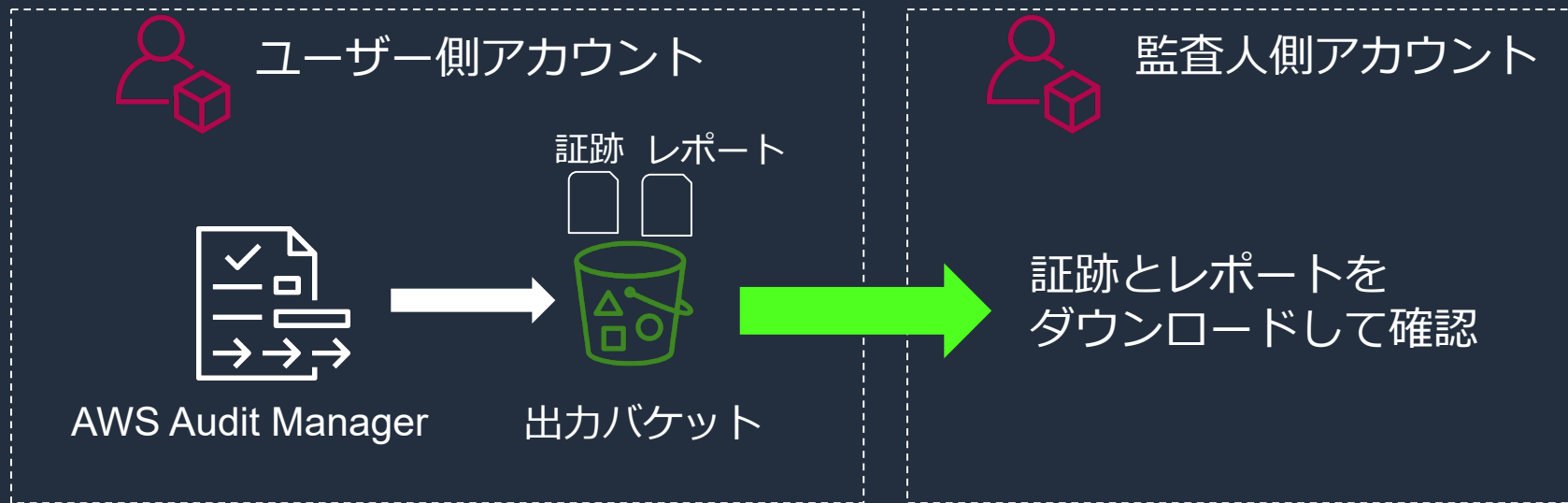
外部監査人が監査する場合のアーキテクチャ パターン 1

ユーザー側の AWS Organizations のメンバーアカウントを払い出し、
移譲アカウントとして設定する



外部監査人が監査する場合のアーキテクチャ パターン 2

ユーザー側で監査人のガイドにより Audit Manager で評価を実行し、作成された証跡/Evidenceと、レポートが出力されている S3バケットへのアクセス権限を 監査人に与える



監査の目的と監査の種類

AWS Audit Manager 概要

AWS Audit Manager 構成要素

AWS Audit Manager アーキテクチャパターン

設定方法、設定例

セキュリティ、料金、制約

パートナー様との協業

まとめ

Audit Manager の初期セットアップ 1

AWS Audit Manager > Set up AWS Audit Manager

Set up AWS Audit Manager

Set up AWS Audit Manager

To get started, select your data encryption preferences. For multiple account support, enable AWS Organizations.

For an optimal AWS Audit Manager experience, enable [AWS Security Hub](#) and [AWS Config](#) to assess security checks and generate evidence.

Permissions

AWS Audit Manager uses a service-linked role to connect to data sources on your behalf, and no action is required by default. To learn more about the type of permissions available in AWS Audit Manager, view [How AWS Audit Manager works with IAM](#).

[View IAM service-linked role permission](#)

Data encryption

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

Customize encryption settings (advanced)
To use the default key, disable this option

Choose an AWS KMS key
This key will be used for encryption instead of the default key.

[Create an AWS KMS key](#)

AWS Organizations - optional

For AWS Audit Manager to support multiple accounts in your organization, choose a delegated administrator for your AWS Organization. [Learn more](#)

Delegated administrator account ID

Audit Managerのデータはデフォルトで暗号化されるが、KMSのCMKで暗号化したい場合には、チェックをして、CMKを指定する

Audit Manager の初期セットアップ 2

Data encryption

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

Customize encryption settings (advanced)
To use the default key, disable this option

Choose an AWS KMS key
This key will be used for encryption instead of the default key.

[Create an AWS KMS key](#)

AWS Organizations - optional

For AWS Audit Manager to support multiple accounts in your organization, choose a delegated administrator for your AWS Organization. [Learn more](#)

Delegated administrator account ID

AWS Config - optional

Allow AWS Audit Manager to access [AWS Config](#) and generate evidence from AWS Config rules. Enabling AWS Config incurs charges.

[Enable on AWS Config](#)

Security Hub - optional

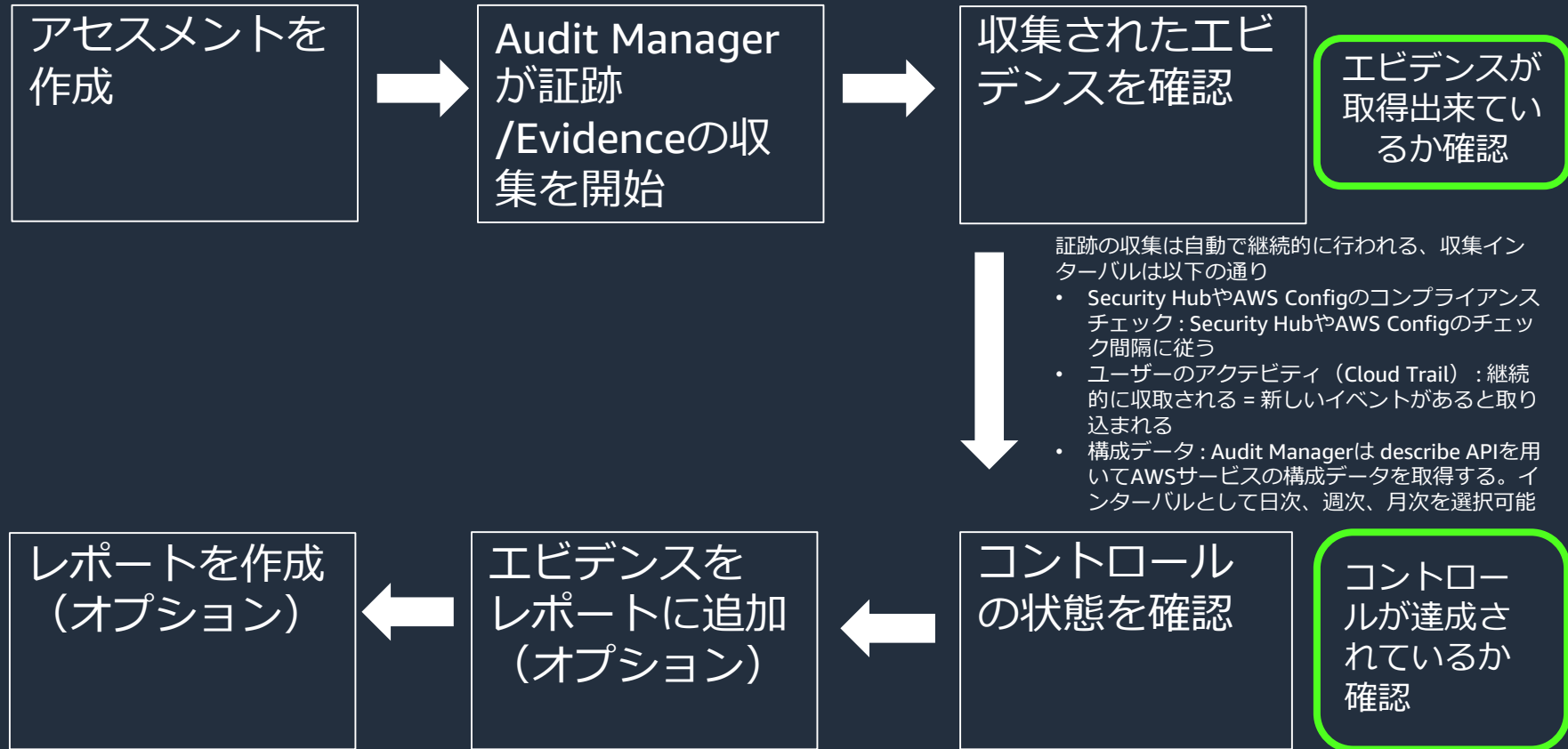
Allow AWS Audit Manager to access [Security Hub](#) and generate evidence from security findings. Enabling Security Hub incurs charges.

[Enable on Security Hub](#)

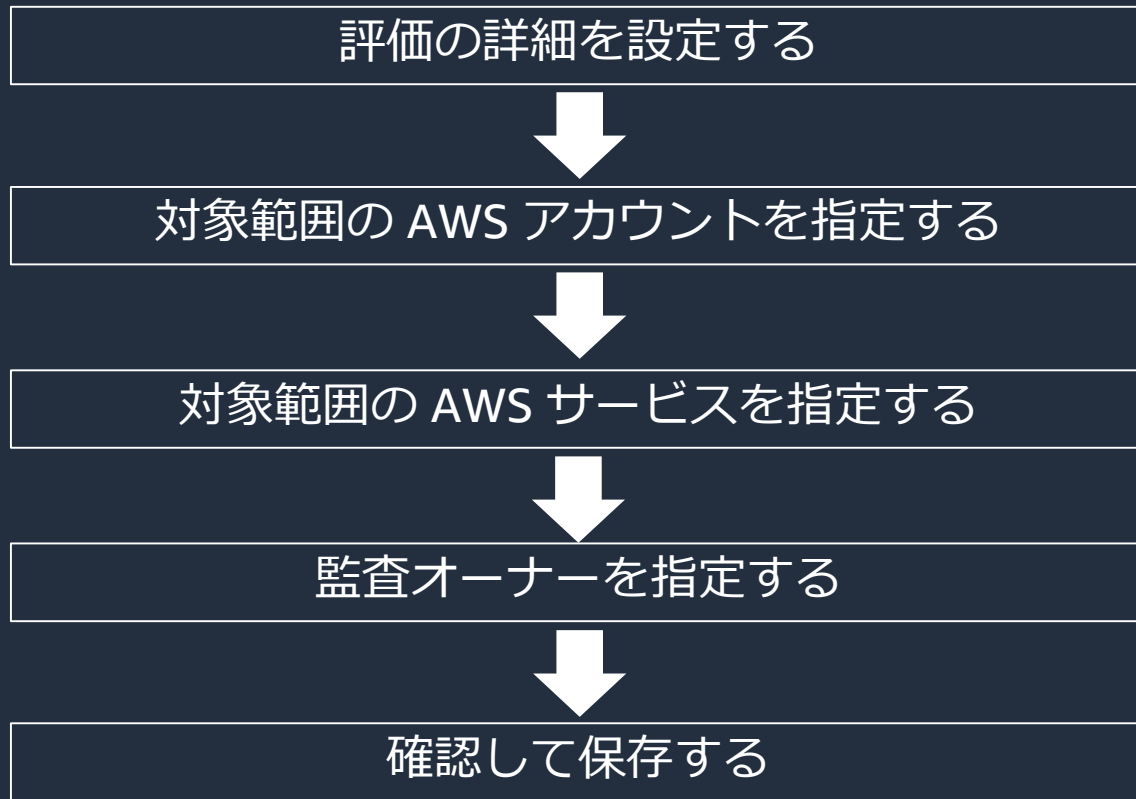
[Complete setup](#)

- AWS Organizations 環境の場合には、委任する管理者のアカウント ID を指定する
- AWS Config や Security Hub は有効化されていないと、AWS Config や Security Hub からの証跡収集が出来ないので、有効化することが推奨

Audit Manager 評価の実行と、レポート作成までの流れ



評価/アセスメントの作成手順



参考 : https://docs.aws.amazon.com/ja_jp/audit-manager/latest/userguide/create-assessments.html

Audit Manager が提供するフレームワークを使った 評価/アセスメントの作成手順 1

Step 1
Specify assessment details

Step 2
Specify AWS accounts in scope

Step 3
Specify AWS services in scope

Step 4
Specify audit owners

Step 5
Review and create

Specify assessment details [Info](#)

Assessment details

Assessment name
PCIDSS Test Assess
Maximum of 300 characters.

Assessment description - *optional*
Describe the assessment in your own words.
Enter assessment description here
Maximum 1000 characters.

Assessment reports destination [Info](#)

Amazon S3 bucket
Select the Amazon S3 bucket in which your assessment reports will be stored.

sat


[Create new bucket](#)

Frameworks (1/14) [Info](#)

Select a standard or custom framework to assist with your audit preparation for this assessment.

Q pc X 1 match < 1 > ⚙

Standard

 **PCI DSS V3.2.1**

The Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 is an information security standard for entities that store, process, and/or transmit cardholder data.

- 評価、アセスメントの名前、説明、レポートを出力する S3 バケットの指定を行う
- フレームワークをキーワードで検索し、指定する
- この例では PCI DSS V3.2.1 を指定している

Audit Manager が提供するフレームワークを使った 評価/アセスメントの作成手順 2

Assessment reports destination [Info](#)

Amazon S3 bucket
Select the Amazon S3 bucket in which your assessment reports will be stored.

sats


[Create new bucket](#)

Frameworks (1/14) [Info](#)

Select a standard or custom framework to assist with your audit preparation for this assessment.

pc 1 match < 1 > ⚙

Standard



PCI DSS V3.2.1

The Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 is an information security standard for entities that store, process, and/or transmit cardholder data.

152 automated controls
513 manual controls
PCI DSS

Tags - optional
Specify up to a total of 50 key-value pairs as tagging for this control.

No tags to display

You can add up to 50 tags.

- 評価/アセスメントに任意のタグを設定可能
- Next を押して次のステップに進む

Audit Manager が提供するフレームワークを使った 評価/アセスメントの作成手順 3

評価/アセスメントの対象となる AWS アカウント ID を指定する

AWS Audit Manager > Assessments > Create assessment

Step 1
[Specify assessment details](#)

Step 2
Specify AWS accounts in scope

Step 3
Specify AWS services in scope

Step 4
Specify audit owners

Step 5
Review and create

Specify AWS accounts in scope [Info](#)

AWS accounts (1/1)

Search by account name, ID or email < 1 >

<input checked="" type="checkbox"/>	Account ID	Account name	Email
<input checked="" type="checkbox"/>	[REDACTED]	-	-

Cancel Previous Next

Audit Manager が提供するフレームワークを使った 評価/アセスメントの作成手順 4

AWS Audit Manager > Assessments > Create assessment

Step 1
Specify assessment details

Step 2
Specify AWS accounts in scope

Step 3
Specify AWS services in scope

Step 4
Specify audit owners

Step 5
Review and create

Specify AWS services in scope [Info](#)

Choose the AWS services to include in the scope of the assessment. AWS Audit Manager will help you audit the usage of resources from the selected services.

AWS services (0/155)

Search by AWS service < 1 2 3 4 5 6 7 >

<input type="checkbox"/>	AWS service	Category	Description
<input type="checkbox"/>	Amazon Elastic Compute Cloud	Compute	Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable computing capacity—literally, servers in Amazon's data centers—that you use to build and host your software systems.
<input type="checkbox"/>	Amazon Simple Storage Service	Storage	Amazon Simple Storage Service (Amazon S3) is storage for objects on the Internet.
<input type="checkbox"/>	Amazon DynamoDB	Database	Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance with automatic and predictable performance and seamless scalability.
<input type="checkbox"/>	Amazon Relational Database Service	Database	Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud.
<input type="checkbox"/>	AWS Lambda	Compute	With AWS Lambda, you can run code without provisioning or managing servers. You pay only for the compute time that you consume—there's no charge when your code isn't running.
<input type="checkbox"/>	Amazon Virtual Private Cloud	Networking and content delivery	Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you've defined.
<input type="checkbox"/>	Amazon Lightsail	Compute	Amazon Lightsail helps developers get started using AWS to build websites or web applications.

- 評価対象とする、AWS サービスを選択する

Audit Manager が提供するフレームワークを使った 評価/アセスメントの作成手順 5

AWS Audit Manager > Assessments > Create assessment

Step 1
Specify assessment details

Step 2
Specify AWS accounts in scope

Step 3
Specify AWS services in scope

Step 4
Specify audit owners

Step 5
Review and create

Specify AWS services in scope [Info](#)

Choose the AWS services to include in the scope of the assessment. AWS Audit Manager will help you audit the usage of resources from the selected services.

AWS services (8/155)

 < 1 2 3 4 5 6 7 >

<input type="checkbox"/>	AWS service	Category	Description
<input checked="" type="checkbox"/>	Amazon Elastic Compute Cloud	Compute	Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable computing capacity—literally, servers in Amazon's data centers—that you use to build and host your software systems.
<input checked="" type="checkbox"/>	Amazon Simple Storage Service	Storage	Amazon Simple Storage Service (Amazon S3) is storage for the internet.
<input checked="" type="checkbox"/>	Amazon DynamoDB	Database	Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability.
<input checked="" type="checkbox"/>	Amazon Relational Database Service	Database	Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud.
<input checked="" type="checkbox"/>	AWS Lambda	Compute	With AWS Lambda, you can run code without provisioning or managing servers. You pay only for the compute time that you consume—there's no charge when your code isn't running.
<input checked="" type="checkbox"/>	Amazon Virtual Private Cloud	Networking and content delivery	Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you've defined.
<input type="checkbox"/>	Amazon Lightsail	Compute	Amazon Lightsail helps developers get started using AWS to build websites or web applications.

Audit Manager が提供するフレームワークを使った 評価/アセスメントの作成手順 6

Step 4
Specify audit owners

Step 5
Review and create

Audit owners (1/19)

Search by user < 1 >

<input type="checkbox"/>	Audit owner	AWS account	IAM type
<input type="checkbox"/>	sharingtestuser		User
<input checked="" type="checkbox"/>	Admin		Role
<input type="checkbox"/>	AWSReservedSSO_AWSAdministratorAccess_ba939f78161d8d7a		Role
<input type="checkbox"/>	AWSReservedSSO_AWSPowerUserAccess_6a1c12c2569f3b8c		Role
<input type="checkbox"/>	AWSReservedSSO_AWSReadOnlyAccess_0b67b4350167ef41		Role
<input type="checkbox"/>	AWSReservedSSO_AWSServiceCatalogAdminFullAccess_111959eaa969551		Role
<input type="checkbox"/>	AWSReservedSSO_AWSServiceCatalogEndUserAccess_7018ae31476b5a83		Role
<input type="checkbox"/>	AwsSecurityAudit		Role
<input type="checkbox"/>	AwsSecurityNacundaAudit		Role
<input type="checkbox"/>	cfn-lint-referee-plugin-DO-NOT-DELETE		Role
<input type="checkbox"/>	GatedGardenAudit		Role
<input type="checkbox"/>	GatedGardenInternalAudit		Role
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>	ResourceConfigurationCollector-DO-NOT-DELETE		Role
<input type="checkbox"/>	ShadowTrooperRole		Role

Cancel Previous Next

- Audit オーナーを指定する、Organizations 構成の場合は、メンバーアカウントのユーザーとロールが選択肢として表示されるのでチェックを行う

Audit Manager が提供するフレームワークを使った 評価/アセスメントの作成手順 7

AWS services (10) [Info](#)

AWS service	Category
AWS Security Hub	Security, identity, and compliance
AWS Config	Management and governance
AWS Identity and Access Management	Security, identity, and compliance
AWS CloudTrail	Management and governance
Amazon Virtual Private Cloud	Networking and content delivery
Amazon DynamoDB	Database
AWS Lambda	Compute
Amazon Relational Database Service	Database
Amazon Simple Storage Service	Storage
Amazon Elastic Compute Cloud	Compute

Step 4: Choose audit owners

Audit owners (1) [Info](#)

Audit owner	AWS account
Admin	[Redacted]

Automatic evidence collection ×

When you create the assessment, AWS Audit Manager automatically starts collecting evidence from the selected AWS accounts and services. Please wait up to 24 hours to view collected evidence.

Cancel Previous **Create assessment**

- 各ステップで指定した内容が表示される
- 確認して Create Assessment を押すと保存される
- アセスメント/評価の実行準備が始まる

評価/アセスメントのステータスの確認 1

- 評価/アセスメントを作成して最初の結果が出るまでは、フレームワークの項目数などにも依存しますが、最大24時間程度かかります
- 実行している評価/アセスメントのステータスを確認することが可能です
- マネージメントコンソールの Assessments を選択すると、現在作成されている評価/アセスメントの一覧が表示される

AWS Audit Manager > Assessments

Assessments [Info](#)

Access all your past and current assessments. You can select an assessment to review the evidence collected and generate an assessment report.

Assessments (1) Edit Delete Create assessment

Search

Assessment	Status	Compliance type	Date created	Last updated
<input type="radio"/> Sample Assessment 1	<input checked="" type="radio"/> Active	CIS Controls	2020年12月11日 3:13 UTC	2020年12月11日 3:13 UTC

アセスメント名を選択すると
詳細な状況が表示される

ステータスは Active と Inactive の2
種類、Active は証拠収集が行われてい
る状態を示す

評価/アセスメントのステータスの確認 2

AWS Audit Manager > Assessments > Sample Assessment 1

Sample Assessment 1 [Info](#)

[Edit](#) [Delete](#) [Update assessment status](#) ▼

Assessment details

Name	Assessment report selection	AWS accounts	Assessment status
Sample Assessment 1	1	1	Active
Description	Total evidence	AWS services	Date created
-	9821	13	2020年12月11日 3:13 UTC
Compliance type	Assessment reports destination	Audit owners	Last updated
CIS Controls	s3://[redacted]	2	2020年12月11日 3:13 UTC

[Controls](#) | [Assessment report selection](#) | [AWS accounts](#) | [AWS services](#) | [Audit owners](#) | [Tags](#) | [Changelog](#)

Control status summary [Info](#)

The control status specifies if AWS Audit Manager is actively collecting evidence for that control. It also indicates the evidence review status for active controls.

Total controls	Reviewed
43	1

各コントロール別の状況が表示される。
Evidence数が1以上になっていれば証跡の収集が成功している

Control sets (16)

Search by control set name or control name

Controls grouped by control set	Control status	Delegated to	Total evidence	Added to assessment report
○ ▶ Applications - Identify (2)	Active	-	303	0
○ ▼ Applications - Protect (4)	Active	-	278	0
3.4 - Deploy Automated Operating System Patch Management Tools	Under review	-	0	0
3.5 - Deploy Automated Software Patch Management Tools	Under review	-	0	0

評価/アセスメントのステータスの確認 3

AWS Audit Manager > Assessments > Sample Assessment 1 > 5.1 - Establish Secure Configurations

5.1 - Establish Secure Configurations [Info](#)

Control details

Control name

5.1 - Establish Secure Configurations

Control description

5.1 Maintain documented security configuration standards for all authorized operating systems and software.

Testing information

AWS Config Rule(s):

AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED

S3_BUCKET_REPLICATION_ENABLED

IAM_ROOT_ACCESS_KEY_CHECK

Learn more at: <https://docs.aws.amazon.com/config/latest/developerguide/managed-rules-by-aws-config.html>

Action plan

-

前のページのコントロールを選択した画面（画面上部抜粋）

Update control status [Info](#)

Change the control status to indicate the status of its review. Controls marked as inactive will no longer collect evidence.

Update control status ▾

Control status

🕒 Under review

評価/アセスメントのステータスの確認 4

Evidence folders (86) [Info](#)

Choose any folder to open it and manage the evidence that was gathered on that day.

Search by evidence folder

Upload manual evidence Remove from assessment report Add to assessment report

Evidence folder	Compliance check	Total evidence
<input checked="" type="radio"/> 2021-03-06	0 issues	3
<input type="radio"/> 2021-03-05	0 issues	3
<input type="radio"/> 2021-03-04	0 issues	3
<input type="radio"/> 2021-03-03	0 issues	2
<input type="radio"/> 2021-03-02	0 issues	3
<input type="radio"/> 2021-03-01	0 issues	3
<input type="radio"/> 2021-02-28	0 issues	3
<input type="radio"/> 2021-02-27	0 issues	3
<input type="radio"/> 2021-02-26	0 issues	3
<input type="radio"/> 2021-02-25	0 issues	3
<input type="radio"/> 2021-02-24	0 issues	3
<input type="radio"/> 2021-02-23	0 issues	3
<input type="radio"/> 2021-02-22	0 issues	3
<input type="radio"/> 2021-02-21	0 issues	3
<input type="radio"/> 2021-02-20	0 issues	3
<input type="radio"/> 2021-02-19	19 issues	22

- 前前ページのコントロールを選択した画面（画面下部抜粋）
- このコントロールでは Config によって証拠の収集が行われているので、毎日証拠が作られている

評価/アセスメントのステータスの確認 5

AWS Audit Manager > Assessments > Sample Assessment 1 > 5.1 - Establish Secure Configurations > 2021-03-06

2021-03-06 [Info](#)

Summary

Evidence folder details

Date	Added to assessment report
2021年3月6日 0:00 UTC	0
Control name	Total evidence
5.1 - Establish Secure Configurations	3
	Resources
	3

Evidence

User Accounts	0	3
Configuration data	0	Compliance check status
		0 issues found
Manual	0	

Evidence (3) [Info](#)

< 1 >

<input type="checkbox"/>	Time	Evidence by type	Compliance check	Data source	Event name	Resources	Assessment report selection
<input type="checkbox"/>	03:22:18 UTC	Compliance check	Compliant	AWS CloudTrail	PutEvaluations	1	No
<input type="checkbox"/>	20:22:23 UTC	Compliance check	Compliant	AWS CloudTrail	PutEvaluations	1	No
<input type="checkbox"/>	08:22:18 UTC	Compliance check	Compliant	AWS CloudTrail	PutEvaluations	1	No

- 前ページの日付を選択した際に表示される画面
- この日は、3回の証跡取得が行われている (AWS Config 上でのチェックが3個セットになっているため)

評価/アセスメントのステータスの確認 5

03:22:18 UTC [Info](#)

Evidence detail

Date and time
2021年3月6日 3:22 UTC

Evidence folder name
2021-03-06

Control name
5.1 - Establish Secure Configurations

Event source
config.amazonaws.com

Event name
PutEvaluations

Data source
AWS CloudTrail

Evidence by type
Compliance check

Compliance check
 **Compliant**

Resources included
1

Attributes
3

- 前ページの時刻を選択すると表示される画面
- この画面が収集した証拠の一番詳細な画面になる
- このコントロールでは Config がデータ収集をしているので、JSON として収集したアカウントID が記録されたものが添付されている

Attributes (3)

Attribute name	Value
ConfigRuleArn	arn:aws:config:ap-northeast-1:164348464951:config-rule/config-rule-pt0sop
configRuleName	iam-root-access-key-check
managedRuleIdentifier	IAM_ROOT_ACCESS_KEY_CHECK

Resources included (1)

ARN	Value	JSON
-	-	View JSON

カスタムコントロールの作成手順

コントロールの詳細を設定する

データソース設定
CloudTrail

データソース設定
Security Hub

データソース設定
Config

データソース設定
API Call snapshots

コントロールが満たされなかった場合の
アクションプランを設定する（オプション）

確認して保存する

参照 : https://docs.aws.amazon.com/ja_jp/audit-manager/latest/userguide/customize-control-from-scratch.html

カスタムコントロールの作成 1

AWS Audit Manager > Control library

Control library [Info](#)

The Control library is the central place for browsing standard controls provided by AWS and managing your custom controls. You can create new custom controls from scratch, or customize standard controls by specifying which data to collect as evidence from your data sources. Visit the [Framework library](#) to add controls to a framework and begin assessing your AWS service usage.

Standard controls | Custom controls

Standard controls (758+)
The search functionality displays 1,000 results at a time. Click through the table pagination to view more.

Customize existing control

Search by control name, data source, or tags

Control name	Data source
<input type="radio"/> 1.0.1 - CloudTrail Instance Events	AWS CloudTrail
<input type="radio"/> 1.0.2 - CloudTrail Volume Events	AWS CloudTrail
<input type="radio"/> 2.2.0 - List Principals and Policies	AWS API calls
<input type="radio"/> 2.2.1 - Describe Networks	AWS API calls
<input type="radio"/> 3.0.0 - Account Summary	Manual
<input type="radio"/> CM-8.a.2 Information System Component Inventory	Manual
<input type="radio"/> CM-8.a.3 Information System Component Inventory	Manual
<input type="radio"/> CM-8.a.4.2 Information System Component Inventory	Manual
<input type="radio"/> CM-8.b.2 Information System Component Inventory	Manual
<input type="radio"/> CM-8(1).1 Information System Component Inventory Updates During Installations / Removals	AWS Config
<input type="radio"/> CM-8(3).a.2 Information System Component Inventory Automated Unauthorized Component Detection	AWS Config
<input type="radio"/> CM-8(3).b.2 Information System Component Inventory Automated Unauthorized Component Detection	AWS API calls

Audit Managerメニューの
Control Library → Create Custom Control で
カスタムコントロール作成画面に入る

カスタムコントロールの作成 2

Specify control details [Info](#)

Provide control and tagging details to help you identify this control in Control library.

Control details

Control name

Enter a unique name for your control.

Maximum 300 characters. (30 given)

Control description - *optional*

Describe the purpose of the custom control.

Maximum 1000 characters. (46 given)

Testing information - *optional* [Info](#)

Description

Provide detailed instructions describing the testing information for this control.

Maximum 1000 characters. (0 given)

Tags - *optional*

Specify up to a total of 50 key-value pairs as tagging for this control.

No tags to display

You can add up to 50 tags.

[Cancel](#)

[Next](#)

カスタムコントロールの作成 3

- AWS Config をデータソースにしたケース
- Config Rules を選択して指定する
- 現状は、標準の Config Rules のみをサポートしており、カスタムのルールはサポートしていない

Configure data sources for this control [Info](#)

You can define up to 10 data sources that map to your AWS service usage. AWS Audit Manager uses these sources to collect evidence such as resource configuration, logs, events, control findings, and rule checks.

[Collapse all](#) [Expand all](#)

▼ **Data source 1** [Remove](#)

Select an evidence collection method
Specify the type of evidence that AWS Audit Manager will collect for your resources from AWS services. If you need help with this step, we recommend that you choose Manual evidence for now and you can edit the custom control after you check with a subject matter expert.

Automated evidence
Evidence that will be collected automatically by AWS Audit Manager.

Manual evidence
Evidence that you will upload manually.

Select an evidence type by mapping to a data source
Specify the type of evidence that AWS Audit Manager will collect for your resources from AWS services.

User activity logs from AWS CloudTrail
Collect evidence generated by AWS CloudTrail logs for the user activity on your resources.

Compliance checks for security findings from AWS Security Hub
Collect evidence generated by AWS Security Hub security checks for your AWS resources.

Compliance checks for resource configurations from AWS Config
Collect evidence generated by AWS Config rules for your AWS resources.

Configuration snapshots from AWS API calls
Collect a daily, weekly, or monthly snapshot of evidence from AWS services for details about the configuration of your AWS resources.

Specify an AWS Config rule
Find the full details for each rule in the [Managed Rules](#) page of the AWS Config user guide.

ALB_WAF_ENABLED ▼

Troubleshooting description - optional
Provide detailed instructions on the actions to take if no evidence is collected from this data source.

Check if AWS WAF exists with ALB.

Maximum 1000 characters. (54 given)

[Add data source](#)

カスタムコントロールの作成 4

- CloudTrail をデータソースに設定した例
- CloudTrail Keywordは一部のキーワードを入力するとマッチングするキーワード（イベント名）が表示される

Edit control data source

You can define up to 10 data sources that map to your AWS service usage. AWS Audit Manager uses these sources to collect evidence such as resource configuration, logs, events, control findings, and rule checks.

▼ Data source 1

Select an evidence collection method
Specify the type of evidence that AWS Audit Manager will collect for your resources from AWS services. If you need help, we recommend that you choose Manual evidence for now and you can edit the custom control after you check with a subject matter expert.

- Automated evidence**
Evidence that will be collected automatically by AWS Audit Manager.
- Manual evidence**
Evidence that you will upload manually.

Select an evidence type by mapping to a data source
Specify the type of evidence that AWS Audit Manager will collect for your resources from AWS services.

- User activity logs from AWS CloudTrail**
Collect evidence generated by AWS CloudTrail logs for the user activity on your resources.
- Compliance checks for security findings from AWS Security Hub**
Collect evidence generated by AWS Security Hub security checks for your AWS resources.
- Compliance checks for resource configurations from AWS Config**
Collect evidence generated by AWS Config rules for your AWS resources.
- Configuration snapshots from AWS API calls**
Collect a daily, weekly, or monthly snapshot of evidence from AWS services for details about the configuration of your AWS resources.

Specify an AWS CloudTrail keyword
Find the full details on the [Viewing Events with CloudTrail Event History](#) page of the AWS CloudTrail user guide.

Choose a keyword

Troubleshooting description - optional
Provide detailed instructions on the actions to take if no evidence is collected from this data source.

Enter a description

Maximum 1000 characters. (0 given)

Search results for 'kms':

- kms_CancelKeyDeletion
- kms_ConnectCustomKeyStore
- kms_CreateAlias
- kms_CreateCustomKeyStore
- kms_CreateGrant
- kms_CreateKey
- kms_DeleteAlias
- kms_DeleteCustomKeyStore
- kms_DeleteImportedKeyMaterial
- kms_DeleteKey

カスタムコントロールの作成 5

- API コールをデータソースに指定したケース
- AWS API 名を選択して指定する
- データソースに CloudTrail を指定した場合との違いは、API コールは設定系や設定参照系のための API パターンに絞られていることである。CloudTrail をデータソースにする場合には、CloudTrail に出現するイベントパターンが全て指定出来る

▼ Data source 1 Remove

Select an evidence collection method
Specify the type of evidence that AWS Audit Manager will collect for your resources from AWS services. If you need help with this step, we recommend that you choose Manual evidence for now and you can edit the custom control after you check with a subject matter expert.

Automated evidence
Evidence that will be collected automatically by AWS Audit Manager.

Manual evidence
Evidence that you will upload manually.

Select an evidence type by mapping to a data source
Specify the type of evidence that AWS Audit Manager will collect for your resources from AWS services.

User activity logs from AWS CloudTrail
Collect evidence generated by AWS CloudTrail logs for the user activity on your resources.

Compliance checks for security findings from AWS Security Hub
Collect evidence generated by AWS Security Hub security checks for your AWS resources.

Compliance checks for resource configurations from AWS Config
Collect evidence generated by AWS Config rules for your AWS resources.

Configuration snapshots from AWS API calls
Collect a daily, weekly, or monthly snapshot of evidence from AWS services for details about the configuration of your AWS resources.

Specify an AWS API to collect configuration snapshot for a specific AWS service
Refer to the specific AWS service's API guide for more details.

Troubleshooting description - optional
Provide detailed instructions on the actions to take if no evidence is collected from this data source.

Maximum 1000 characters. (0 given)

Custom control frequency
Specify the desired frequency for evidence generation.

Daily

Weekly

Monthly

Add data source

You can add up to 9 more data sources.

Cancel Previous Next

カスタムコントロールの作成 6

- Security Hub をデータソースにしたケース
- Security Hub のルールを選択して指定する

Configure data sources for this control [info](#)

You can define up to 10 data sources that map to your AWS service usage. AWS Audit Manager uses these sources to collect evidence such as resource configuration, logs, events, control findings, and rule checks.

[Collapse all](#) [Expand all](#)

▼ **Data source 1** [Remove](#)

Select an evidence collection method
Specify the type of evidence that AWS Audit Manager will collect for your resources from AWS services. If you need help with this step, we recommend that you choose Manual evidence for now and you can edit the custom control after you check with a subject matter expert.

Automated evidence
Evidence that will be collected automatically by AWS Audit Manager.

Manual evidence
Evidence that you will upload manually.

Select an evidence type by mapping to a data source
Specify the type of evidence that AWS Audit Manager will collect for your resources from AWS services.

User activity logs from AWS CloudTrail
Collect evidence generated by AWS CloudTrail logs for the user activity on your resources.

Compliance checks for security findings from AWS Security Hub
Collect evidence generated by AWS Security Hub security checks for your AWS resources.

Compliance checks for resource configurations from AWS Config
Collect evidence generated by AWS Config rules for your AWS resources.

Configuration snapshots from AWS API calls
Collect a daily, weekly, or monthly snapshot of evidence from AWS services for details about the configuration of your AWS resources.

Specify an AWS Security Hub rule
Find the full details for each CIS and PCI DSS check in the [Security standards and controls](#) page of the AWS Security Hub user guide.

1.1 ▼

Troubleshooting description - optional
Provide detailed instructions on the actions to take if no evidence is collected from this data source.

Check who used root user.

Maximum 1000 characters. (26 given)

[Add data source](#)

You can add up to 9 more data sources.

[Cancel](#) [Previous](#) [Next](#)

カスタムコントロールの作成 7

- データソースは 10個まで 1つのコントロールに指定可能
- データソースを指定すると確認画面が表示される

Review and create [Info](#)

Step 1: Control details Edit

Control details

Control name
CustomControlforInternalAudit1

Control description
This is the custom control for internal audit.

Testing information

Description
-

Tags (1)

Key	Value
purpose	internalaudit

Step 2: Configure data sources for this control Edit

Data source (1)

Name	Data source	Attribute	Frequency
Data source 1	AWS Config	ALB_WAF_ENABLED	-

カスタムコントロールの作成 8

- 内容を確認して、Create custom control ボタンを押すと作成が完了する

Testing information

Description
-

Tags (1)

Key	Value
purpose	internalaudit

Step 2: Configure data sources for this control Edit

Data source (1)

Name	Data source	Attribute	Frequency
Data source 1	AWS Config	ALB_WAF_ENABLED	-

Step 3: Define action plan Edit

Action plan

Title
Enable AWS WAF and attached to ALB

Action plan instructions
-

Cancel Previous Create custom control

カスタムコントロールの作成 9

Successfully created CustomControlforInternalAudit1 Add control to framework

Add your new control to a custom framework so that you can create an assessment and begin collecting evidence.

[AWS Audit Manager](#) > [Control library](#) > CustomControlforInternalAudit1

CustomControlforInternalAudit1

[Edit](#) [Delete](#) [Customize existing control](#)

Summary

Control name CustomControlforInternalAudit1	Control sources 1	Created by [Redacted]
Control type Custom	Tags 1	Date created 2021年3月4日 8:16 UTC
		Last updated 2021年3月4日 8:16 UTC

[Control details](#) | [Tags](#)

Control details

Control name
CustomControlforInternalAudit1

Control description
This is the custom control for internal audit.

Testing information

Description
-

Data sources (1)

Name	Data source	Attribute	Frequency
------	-------------	-----------	-----------

カスタムフレームワークの作成手順

フレームワークの詳細を設定する



コントロールをコントロールセットから追加する



確認して保存する

カスタムフレームワークの作成 1

AWS Audit Manager > Framework library

Disclaimer
AWS Audit Manager is designed to assist in collecting evidence that is relevant for verifying compliance with certain compliance frameworks and regulations, but it does not assess your compliance itself. The evidence collected through AWS Audit Manager therefore may not include all information about your AWS usage needed for audits. AWS Audit Manager is not a substitute for legal counsel or compliance experts.

Framework library Info

The Framework library is the central place for browsing standard frameworks and managing custom frameworks. You can create new frameworks from scratch, or customize and modify an existing framework per your needs. Visit the [Control library](#) to define custom controls to use in your frameworks.

Standard frameworks | Custom frameworks

Standard frameworks (14) Create assessment from framework **Create custom framework**

Search by control name, data source, or tags

	Framework name ▲	Compliance type ▼	Control sets	Controls
<input type="radio"/>	AWS Audit Manager Sample Framework	AWS Audit Manager Sample Framework	3	5
<input type="radio"/>	AWS Control Tower Guardrails	AWS Control Tower Guardrails	5	14
<input type="radio"/>	AWS License Manager	AWS License Manager	6	27
<input type="radio"/>	AWS Operational Best Practices	AWS Operational Best Practices	20	52
<input type="radio"/>	CIS Benchmark for CIS Amazon Web Services Foun...	CIS	4	36
<input type="radio"/>	CIS Benchmark for CIS Amazon Web Services Foun...	CIS	4	49
<input type="radio"/>	CIS Controls v7.1 IG1	CIS Controls	16	43
<input type="radio"/>	FedRAMP Moderate Baseline by Allgress	FedRAMP	325	1211
<input type="radio"/>	GDPR	GDPR	10	771

カスタムフレームワークの作成 2

>Create new framework

Specify framework details [info](#)

Provide details to help you find this framework in the Framework library.

Framework detail

Framework name

Maximum 300 characters. (31 given)

Compliance type - optional
Enter the compliance standard that your framework supports.

Maximum 100 characters. (13 given)

Description - optional
Provide a detailed description of the purpose of this framework.

Maximum 1000 characters. (0 given)

Tags - optional

Specify up to a total of 50 key-value pairs as tagging for this control.

No tags to display

You can add up to 50 tags.

Cancel

カスタムフレームワークの作成 3

Specify the controls in the control sets [Info](#)

Specify which controls you want to add to your framework and how you want to organize them. The control sets that you specify will determine how AWS Audit Manager collects evidence for this assessment.

[Collapse all](#) [Expand all](#)

▼ **AuthenticationCheck** [Remove control set](#)

Specify a control set name

Control set name

Maximum 300 characters.

Add a new control to the control set

Select control type

Specify whether you want to add a standard or custom control to the control set.

Available custom controls (1/2)

Select and filter the list of existing custom controls to select and add to this control set.

< 1 > ⚙

<input type="checkbox"/>	Control name	Tags	Data source	Date created	Last updated
<input type="checkbox"/>	Encryption at rest	View tags	AWS Config	2021年1月12日 UTC	2021年1月12日 UTC
<input checked="" type="checkbox"/>	CustomControlforInternalAudit1	View tags	AWS Config	2021年3月4日 UTC	2021年3月4日 UTC

Review the selected controls in the control set

Add to control set ✕

Are you sure you want to add 1 custom control to the control set **AuthenticationCheck**?

[Cancel](#) [Add to control set](#)

[Add to control set](#)

カスタムフレームワークの作成 4

Maximum 300 characters.

Add a new control to the control set

Select control type
Specify whether you want to add a standard or custom control to the control set.

Custom controls

Available custom controls (1/2)

Select and filter the list of existing custom controls to select and add to this control set.

Search by control name, data source, or tags

< 1 > ⚙

<input type="checkbox"/>	Control name	Tags	Data source	Date created	Last updated
<input type="checkbox"/>	Encryption at rest	View tags	AWS Config	2021年1月12日 UTC	2021年1月12日 UTC
<input checked="" type="checkbox"/>	CustomControlforInternalAudit1	View tags	AWS Config	2021年3月4日 UTC	2021年3月4日 UTC

Review the selected controls in the control set

Selected controls (1)

You can add up to 25 standard or custom controls to this control set.

Remove control

< 1 >

<input type="checkbox"/>	Control name	Type
<input type="checkbox"/>	CustomControlforInternalAudit1	Custom

Add control set

You can add 9 more control sets.

Cancel Previous **Next**

カスタムフレームワークの作成 5

ary > Create new framework

Review and create [Info](#)

Step 1: Specify framework details Edit

Framework detail

Framework name
CustomFrameworkforInternalAudit

Compliance type
InternalAudit

Description
-

Tags (0)

Key	Value
No tags	

Step 2: Select controls to add to control set Edit

Selected controls (2)

Controls grouped by control set	Type	Data source
▼ AuthenticationCheck	-	-
CustomControlforInternalAudit1	Custom	AWS Config

Cancel Previous Create custom framework

手動の証跡/エビデンスのアップロード

AWS Audit Manager がサポートしていない AWS リソースや、運用体制など AWS 上の設定などで証跡が取得出来ない項目について、手動で証跡となるファイルをアップロードしておくことが可能

手動の証跡アップロードの例

このコントロールは端末側の監査項目なので、Audit Manager は証跡を収集出来ないため、手動コントロールとなっている、Upload manual evidence を押すと Amazon S3 バケットからファイルをアップロード出来る

The screenshot displays the AWS Audit Manager interface for control 16.11 - Lock Workstation Sessions After Inactivity. The page is divided into several sections:

- Control details:** Shows the control name, description, testing information, and action plan.
- Update control status:** Includes a button to update the control status and a dropdown menu currently set to "Under review".
- Evidence folders:** A tabbed interface with "Evidence folders" selected. It shows "Evidence folders (0)" and a search bar. A green box highlights the "Upload manual evidence" button.
- Table:** A table with columns for "Evidence folder", "Compliance check", "Total evidence", and "Assessment report selection". The table is currently empty, with a message "No collected evidence for this control" at the bottom.

アップロード元のオブジェクトの指定

[AWS Audit Manager](#) > [Assessments](#) > [Sample Assessment 1](#) > [16.11 - Lock Workstation Sessions After Inactivity](#) > Upload manual evidence

Upload manual evidence

You can upload manual evidence from any [Amazon S3](#) bucket by specifying the S3 URI of the evidence. You can find and copy the S3 URI from the Amazon S3 console, and paste the URI here to upload the evidence.

Upload from Amazon S3

Specify S3 URI

Cancel

Upload

評価レポート

- 必要に応じて PDF 形式の評価レポートを作成することが可能
- 評価レポートに含まれる情報
 - 評価のサマリー: 評価日、評価対象のサービス、フレームワーク、含まれるコントロール
 - 証跡の内容 (証跡 1 つ 1 つが PDF ファイルとなってリンクが埋め込まれる)

Summary for Assessment Report: AssessmentReport2

Assessment Details

Assessment Report Name: AssessmentReport2

Report Creation Date: Mar 8, 2021 at 10:25:34 AM GMT

Assessment Name: Sample Assessment 1

Assessment Start Date: Dec 11, 2020 at 3:13:05 AM GMT

Assessment Description: -

AWS Accounts In Scope: [REDACTED]

AWS Services In Scope: Amazon CloudWatch, AWS AppConfig, Amazon API Gateway, AWS Amplify, AWS Security Hub, AWS Config, AWS Identity and Access Management, AWS CloudTrail, Amazon Virtual Private Cloud, AWS Lambda, Amazon Relational Database Service, Amazon Simple Storage Service, Amazon Elastic Compute Cloud

Framework Name: CIS Controls v7.1 IG1

Controls: 2

Total Evidence: 75

Evidence

Control: 13.1 - Maintain an Inventory of Sensitive Information

- Evidence Folder: 2020-12-11
 - [1607674679000_ec94f990e3.pdf](#)

Control: 2.2 - Ensure Software is Supported by Vendor

- Evidence Folder: 2021-02-25
 - [1614254428000_3c59e4d023.pdf](#)
 - [1614232762000_c23eeb67cd.pdf](#)
 - [1614220998000_527739233d.pdf](#)
 - [1614254431000_b53da5237f.pdf](#)
 - [1614222991000_cb7a934a8e.pdf](#)
 - [1614221001000_11989rcf5d.pdf](#)
 - [1614223144000_932f5339d7.pdf](#)
 - [1614232770000_77a1fe9156.pdf](#)
 - [1614238787000_7af289a82c.pdf](#)
 - [1614249559000_2c90953b58.pdf](#)
 - [1614238787000_22594e84b8.pdf](#)
 - [1614222902000_d5e6d6a11f.pdf](#)
 - [1614232554000_c326da10e8.pdf](#)
 - [1614237342000_8f74d52dc7.pdf](#)
 - [1614223443000_fc0a0a548f.pdf](#)
 - [1614224751000_836ed33bb7.pdf](#)
 - [1614222932000_84c3460c32.pdf](#)
 - [1614253889000_c13510b3f5.pdf](#)
 - [1614223144000_e87bea1a19.pdf](#)
 - [1614237345000_25e2444f4d.pdf](#)
 - [1614232653000_d9c0764964.pdf](#)
 - [1614232653000_ca8ae303a1.pdf](#)

Evidence: 7b51e8de-915c-4110-8d86-fa9e6d052614

Evidence Details

Control: 2.2 - Ensure Software is Supported by Vendor

Author: AWS Audit Manager

Description: Automated Audit Manager evidence for account: 164348464951 from source: AWS CloudTrail

Event AWS Account ID: [REDACTED]951

Event Name: PutEvaluations

Event Time: Feb 25, 2021 at 7:33:45 AM GMT

AWS Account ID: [REDACTED]951

AWS Organization: -

AWS Service Source: config.amazonaws.com

IAM Entity ID: arn:aws:iam::[REDACTED]:role/AWSManagedInstanceProfileForConfig/config.amazonaws.com

Evidence Type: Compliance check

Compliance Check: NOT_APPLICABLE

Attributes

configRuleName: *securityhub-ec2-managedinstance-association-compliance-status-check-c683f7*

ConfigRuleArn: *arn:aws:config:[REDACTED]:464951:config-rule/laws-service-rule/securityhub.amazonaws.com/config-rule-witbul*

configRuleInputParameters: *{}*

managedRuleIdentifier:

EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK

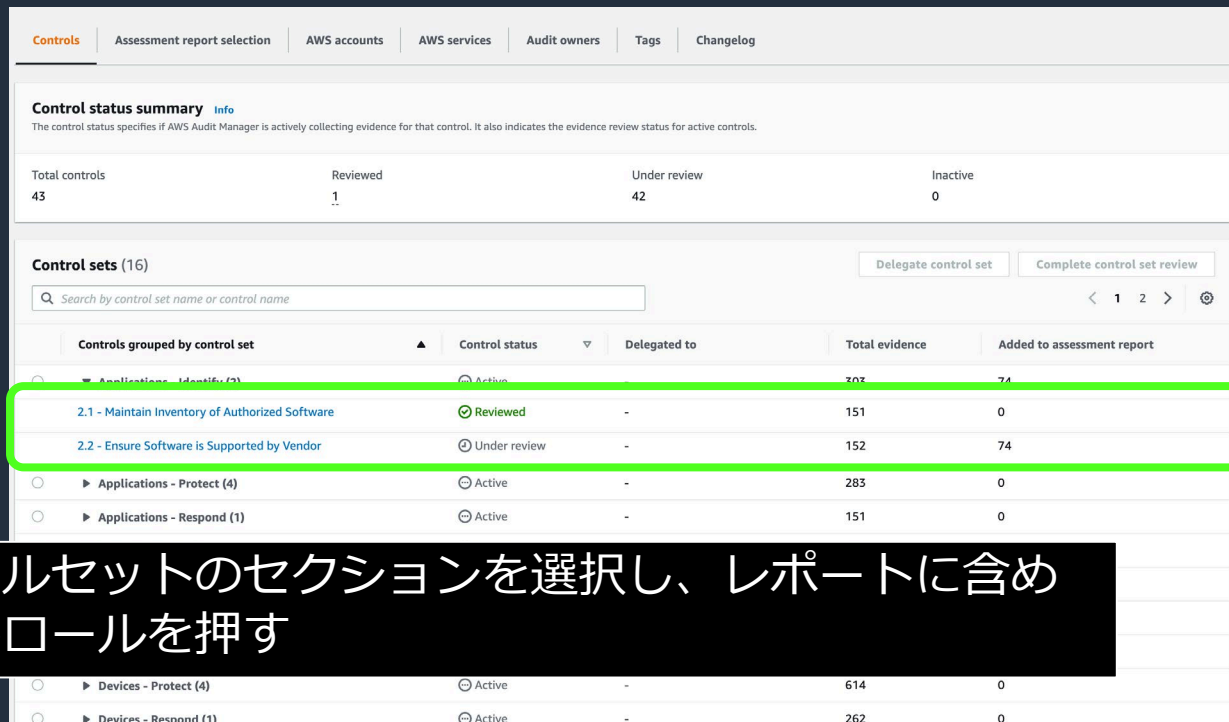
Resources Included

ARN: Value:

*[{"complianceResourceType": "AWS::SSM::AssociationCompliance", "complianceResourceId": "AWS::SSM::ManagedInstanceInventory/fi-022776693234ce15"}]

評価レポートの作成 1

AWS マネージメントコンソールの Audit Manger → Assessment → レポートを作りたい Assessment を選択する



Control status summary Info

The control status specifies if AWS Audit Manager is actively collecting evidence for that control. It also indicates the evidence review status for active controls.

Total controls	Reviewed	Under review	Inactive
43	1	42	0

Control sets (16)

Search by control set name or control name

Controls grouped by control set	Control status	Delegated to	Total evidence	Added to assessment report
Applications - Identify (2)	Active	-	302	74
2.1 - Maintain Inventory of Authorized Software	Reviewed	-	151	0
2.2 - Ensure Software is Supported by Vendor	Under review	-	152	74
Applications - Protect (4)	Active	-	283	0
Applications - Respond (1)	Active	-	151	0
Devices - Protect (4)	Active	-	614	0
Devices - Respond (1)	Active	-	262	0

コントロールセットのセクションを選択し、レポートに含めたいコントロールを押す

評価レポートの作成 2

EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK
EC2_INSTANCE_MANAGED_BY_SSM

Learn more at: <https://docs.aws.amazon.com/config/latest/developerguide/managed-rules-by-aws-config.html>

Action plan
-

Update control status [info](#)
Change the control status to indicate the status of its review. Controls marked as inactive will no longer collect evidence.

証跡フォルダーを選択し、
Add To assessment report ボタンを押す
確認画面が出るので
Add To assessment report ボタンを押す

Add to assessment report ×

Are you sure you want to add the evidence folder, 2021-02-25, to the assessment report?

Cancel **Add to assessment report**

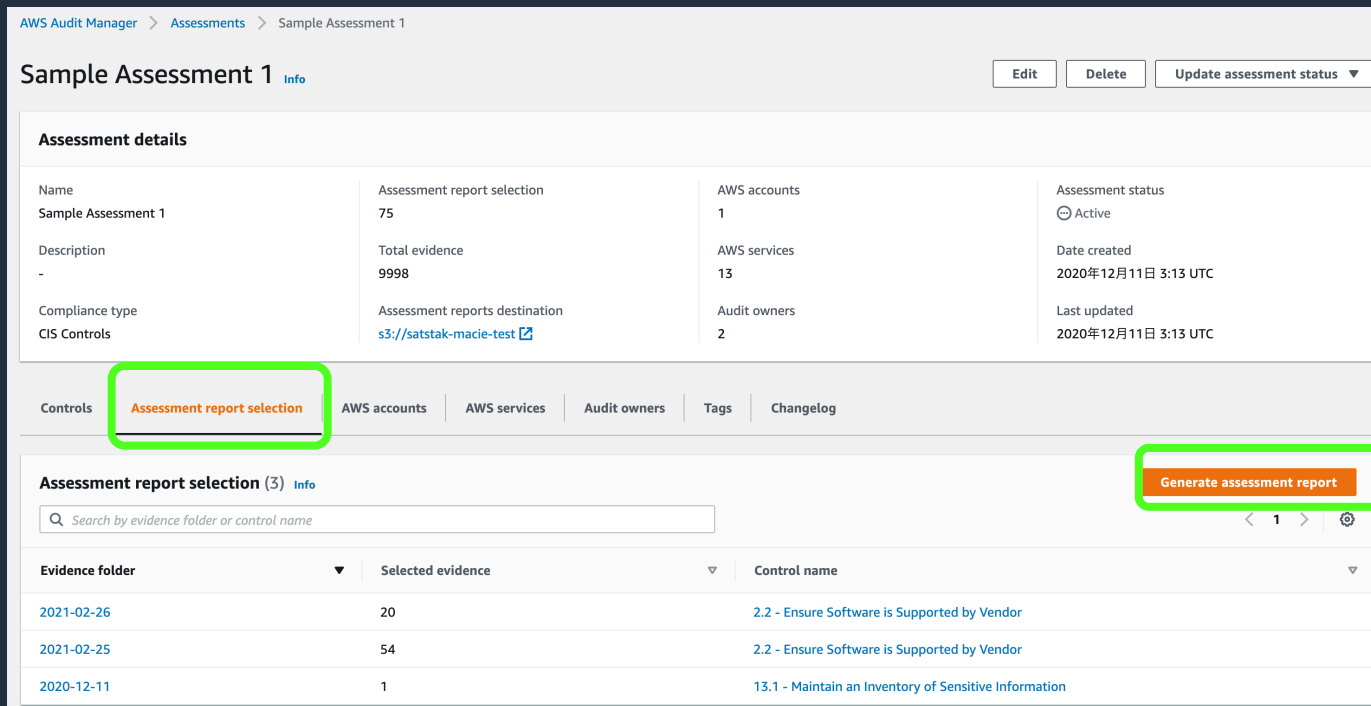
al evidence Remove from assessment report **Add to assessment report**

Search by evidence folder

Evidence folder	Compliance check	Total evidence	Assessment report selection
<input type="radio"/> 2021-03-03	0 issues	2	0
<input type="radio"/> 2021-02-26	12 issues	20	20
<input checked="" type="radio"/> 2021-02-25	13 issues	54	0
<input type="radio"/> 2021-02-19	13 issues	20	0
<input type="radio"/> 2021-02-17	0 issues	8	0
<input type="radio"/> 2021-02-09	2 issues	4	0
<input type="radio"/> 2021-02-07	2 issues	4	0
<input type="radio"/> 2021-02-05	0 issues	8	0

評価レポートの作成 3

アセスメントの画面で、Assessment report selection タブを選択し、右側にある Generate assessment report ボタンを押すとレポートが生成される



Assessment details

Name	Assessment report selection	AWS accounts	Assessment status
Sample Assessment 1	75	1	Active
Description	Total evidence	AWS services	Date created
-	9998	13	2020年12月11日 3:13 UTC
Compliance type	Assessment reports destination	Audit owners	Last updated
CIS Controls	s3://satstak-macie-test	2	2020年12月11日 3:13 UTC

Controls | **Assessment report selection** | AWS accounts | AWS services | Audit owners | Tags | Changelog

Assessment report selection (3)

Search by evidence folder or control name

Evidence folder	Selected evidence	Control name
2021-02-26	20	2.2 - Ensure Software is Supported by Vendor
2021-02-25	54	2.2 - Ensure Software is Supported by Vendor
2020-12-11	1	13.1 - Maintain an Inventory of Sensitive Information

評価レポートの作成 4

Generate assessment report

Provide a name and description to generate an assessment report.

Assessment report name

Use an underscore (_) or hyphen (-) to separate words. Spaces are not allowed. Maximum of 300 characters.

Description

Provide a description for this assessment report.

Maximum 1000 characters. (0 given)

Assessment report details

Assessment name
Sample Assessment 1

Assessment report selection
75

Assessment reports destination
s3://[redacted]st [🔗](#)

Cancel Generate assessment report

レポートの名前と説明を入力し、
保管される Amazon S3 バケットを確認して
Generate assessment report ボタンを押す

評価レポートの作成 5

Audit Manager → Assessment reports のメニューより作成済みのレポートを選択してダウンロードすることが可能

AWS Audit Manager > Assessment reports

Assessment reports Info

Access your generated assessment reports passed from launched assessments needed for your compliance framework.

Assessment reports (1/4) Delete Download

Filter assessment reports

Assessment report	Status	Assessment	Date created	Author	Description
<input checked="" type="radio"/> AssessmentReport2	✔ Generated	Sample Assessment 1	2021年3月8日 10:25 UTC	Admin	-
<input type="radio"/> samplereport2	✔ Generated	Sample Assessment 1	2021年3月1日 0:37 UTC	Admin	-
<input type="radio"/> Assessment_report_2	✔ Generated	Sample Assessment 1	2021年2月11日 22:48 UTC	Admin	This is Report No2.
<input type="radio"/> samplereport1	✔ Generated	Sample Assessment 1	2020年12月14日 4:24 UTC	Admin	this is just sample

評価レポートの作成 6

- レポートは ZIP ファイルとしてダウンロードされる
- ZIP ファイルの中には、レポートサマリーの PDF と各証跡の PDF ファイルが日付ディレクトリの中に入っています
- digest.txt は このZIP ファイルの中の各ファイルのハッシュ値が入っています (sha-384)

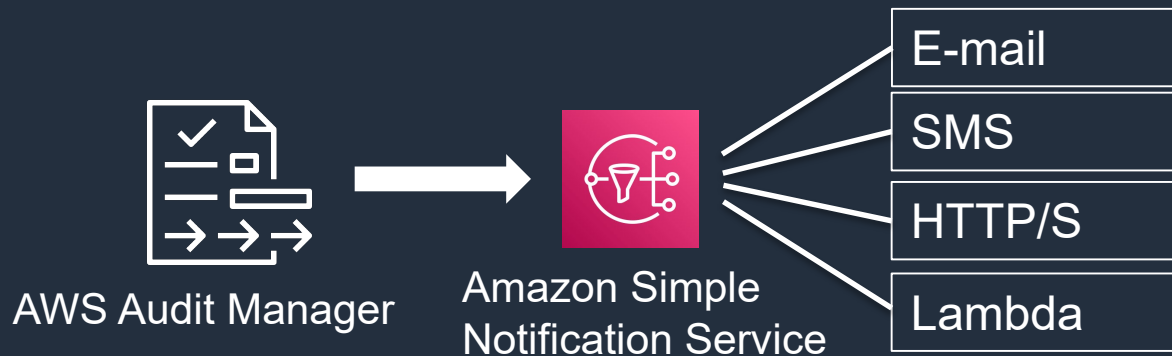
名前	変更日	サイズ	種類
▼  ce5887f3d9-Assessment	今日 19:26	--	フォルダ
 AssessmentReportSummary.pdf	今日 10:25	21 KB	PDF書類
▼  d9e18-22EnsureSoftwar	今日 19:26	--	フォルダ
▶  2021-02-25	今日 19:26	--	フォルダ
▶  2021-02-26	今日 19:26	--	フォルダ
 digest.txt	今日 10:25	17 KB	標準テキ
▼  f177b-131MaintainanIn	今日 19:26	--	フォルダ
▶  2020-12-11	今日 19:26	--	フォルダ

Audit Manager からの通知

以下の場合、Audit Manager は SNS に通知を飛ばす

- コントロールセットと証跡を管理オーナーが他のユーザーに移譲した場合
- コントロールセットのレビューを委任者が完了した場合

通知を送るためには、Audit ManagerのサービスリンクロールにAmazon SNS トピックに対する権限が必要



監査の目的と監査の種類

AWS Audit Manager 概要

AWS Audit Manager 構成要素

AWS Audit Manager アーキテクチャパターン

設定方法、設定例

セキュリティ、料金、制約

パートナー様との協業

まとめ

Audit Manager のセキュリティ 1

保管データ	種別	格納場所	暗号化方法
	メタデータ	Amazon S3	AWS所有のCMKでSSE-KMSで暗号化される
		DynamoDB	AWS所有のCMKでサーバーサイド暗号化される
	コンテンツ	Amazon S3	カスタマーマネージドのCMKでSSE-KMSで暗号化 もしくは、AWS所有のCMKでSSE-S3で暗号化
		Dynamo DB	カスタマーマネージドのCMK か AWS 所有のCMK でクライアントサイド暗号化される（CMKの設定は 選択可能）
Amazon S3 に置かれる 評価レポー ト	カスタマーマネージドのCMKでSSE-KMSで暗号化、もしくは、AWS所有のCMKで SSE-S3で暗号化（選択可能）		

Audit Manager のセキュリティ 2

転送時の暗号化	Audit Manager と他の AWS サービス間の通信は全て TLS で暗号化される
VPC エンドポイントのサポート	インターフェース VPC エンドポイント (AWS PrivateLink) をサポートしている
連携する AWS サービスへのアクセス	Audit Manager のサービスリンクロールで連携する AWS サービスにアクセスする
CloudTrail への記録	API コールの CloudTrail への記録をサポート
変更ログの記録	評価やコントロールセットの変更を内部に記録して表示する機能がある
保管されたレポートの整合性確認	Audit Manager が作成したレポートにはチェックサムがついており、不正に改ざんされていないか確認することが可能

利用料金

各リージョンのアカウントあたりAudit Manager リソース評価 1,000 件ごとに 1.25USD
(東京リージョン)

リソースとは、Amazon EC2 や Amazon S3 などのサービスに対して実行する評価の対象で、EC2 だとスナップショット、ユーザーのアクティビティ (CloudTrail)、インスタンスなどが1つずつカウントされる

Audit Manager のアセスメント/評価は設定すると毎日実行されるので、Audit Manager の監査対象としたリソースの数 X 30 がヶ月のリソース評価の合計となる

Audit Manager のデータソースとなる、AWS Config , AWS Security Hub, AWS CloudTrail の利用料金は Audit Manager の利用料金とは別途必要

無料利用枠 : 利用開始から60日間、月あたり 35,000件までのリソース評価は無料

参照 : <https://aws.amazon.com/jp/audit-manager/pricing/>

制約

- 2021年3月9日現在、Audit Manager の UI や、生成されるレポートは英語のみとなっています
- クォータ
 - アカウントごとのアクティブな評価/アセスメントの数 : 100
 - アカウントごとのカスタムコントロール数 : 500
 - アカウントごとのカスタムフレームワークの数 : 100
- Audit Manager と連携するサービスが有効化されていない場合の動作
 - AWS Config : AWS Config が有効化されていないと、AWS Config から証跡を得るコントロールは証跡を収集しません

よくあるご質問

- AWS Cloud Trail, AWS Config 等を今単体で使っているが、Audit Manager も追加で導入したほうが良いのか？
 - 内部監査、外部監査などの監査対応が必要な場合に、Audit Managerが必要になります
 - 監査対応が要件としてない場合には、発見的統制のソリューションである、GuardDuty, Security Hub, AWS Config などの組み合わせで十分です
- Audit Manager はリージョンごとのサービスですか？
 - Audit Manager リージョンごとのサービスです
 - 複数のリージョンで利用するためには、各リージョンで Audit Manager を有効化する必要があります
 - 現状リージョンまたぎの証跡の収集は出来ません

監査の目的と監査の種類

AWS Audit Manager 概要

AWS Audit Manager 構成要素

AWS Audit Manager アーキテクチャパターン

設定方法、設定例

セキュリティ、料金、制約

パートナー様との協業

まとめ

パートナー様との協業

監査を実際に担当されるパートナー様との協業が重要と考えており、グローバルでは既に Audit Manager をサポート頂くパートナー様との協業が始まっています。日本でも Audit Manager のパートナー様を募集しております



監査の目的と監査の種類

AWS Audit Manager 概要

AWS Audit Manager 構成要素

AWS Audit Manager アーキテクチャパターン

設定方法、設定例

セキュリティ、料金、制約

パートナー様との協業

まとめ

まとめ

- AWS Audit Manager は監査作業、特に証跡/エビデンスの収集を効率化するサービス
 - 監査そのものを実現するサービスではない
- AWS 上のリソース、CloudTrail、AWS Config、Security Hub、EC2, S3, VPCなどから監査に必要な証跡を自動的に収集し、証跡として保管する
- 多くの業界標準の認証や監査のフレームワーク、コントロールをサービスの一部として提供（PCI DSS, FedRAMP, HIPAA 等）
- お客様独自のカスタムフレームワーク、カスタムコントロールの作成も可能
- 監査においては、専門家である監査人の知見が重要なので、AWS では監査に Audit Manager を活用してくれるパートナー様との協業を重視しており、パートナー様を募集しています

参考情報

- AWS Audit Manager ユーザーガイド
<https://docs.aws.amazon.com/audit-manager/latest/userguide/what-is.html>
- AWS Audit Manager API ガイド
<https://docs.aws.amazon.com/audit-manager/latest/APIReference/Welcome.html>

Q&A

お答えできなかったご質問については

AWS Japan Blog 「<https://aws.amazon.com/jp/blogs/news/>」にて

後日掲載します。

AWS の日本語資料の場所「AWS 資料」で検索



日本担当チームへお問い合わせ サポート 日本語 ▾ アカウント ▾

コンソールにサインイン

製品 ソリューション 料金 ドキュメント 学習 パートナー AWS Marketplace その他 🔍

AWS クラウドサービス活用資料集トップ

アマゾン ウェブ サービス (AWS) は安全なクラウドサービスプラットフォームで、ビジネスのスケールと成長をサポートする処理能力、データベースストレージ、およびその他多種多様な機能を提供します。お客様は必要なサービスを選択し、必要な分だけご利用いただけます。それらを活用するために役立つ日本語資料、動画コンテンツを多数ご提供しております。(本サイトは主に、AWS Webinar で使用した資料およびオンデマンドセミナー情報を掲載しています。)

[AWS Webinar お申込 »](#)

[AWS 初心者向け »](#)

[業種・ソリューション別資料 »](#)

[サービス別資料 »](#)

<https://amzn.to/JPArchive>



AWS Well-Architected 個別技術相談会

毎週“W-A個別技術相談会”を実施中

- AWSのソリューションアーキテクト(SA)に
対策などを相談することも可能

• 申込みはイベント告知サイトから

(<https://aws.amazon.com/jp/about-aws/events/>)

AWS イベント

で[検索]



ご視聴ありがとうございました

AWS 公式 Webinar
<https://amzn.to/JPWebinar>



過去資料
<https://amzn.to/JPArchive>

