# [AWS Black Belt Online Seminar]
# AWS Audit Manager

サービスカットシリーズ

Security Solutions Architect
髙橋 悟史
2021年3月9日

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

過去資料
https://amzn.to/JPArchive

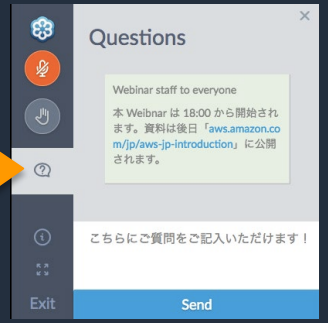
# AWS Black Belt Online Seminar とは

**「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います。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

髙橋　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

# 本日お話する内容

- 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

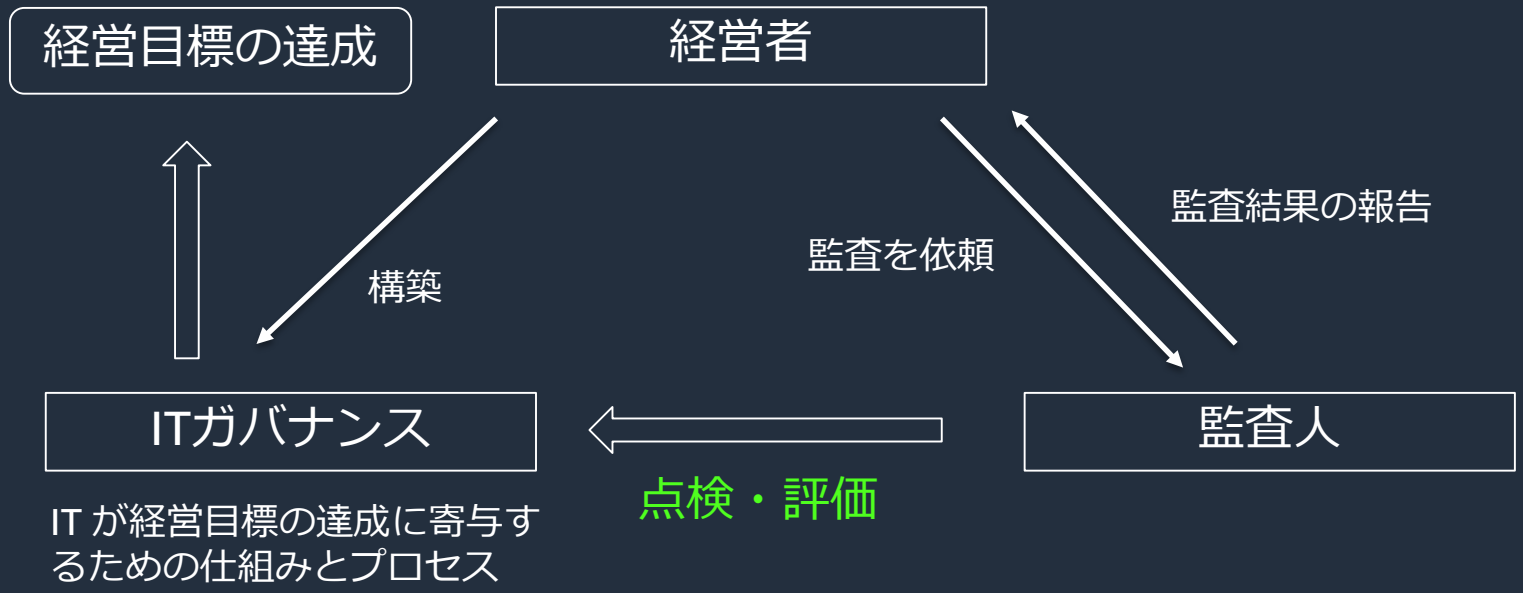
設定方法、設定例

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<br>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<br>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



aws

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

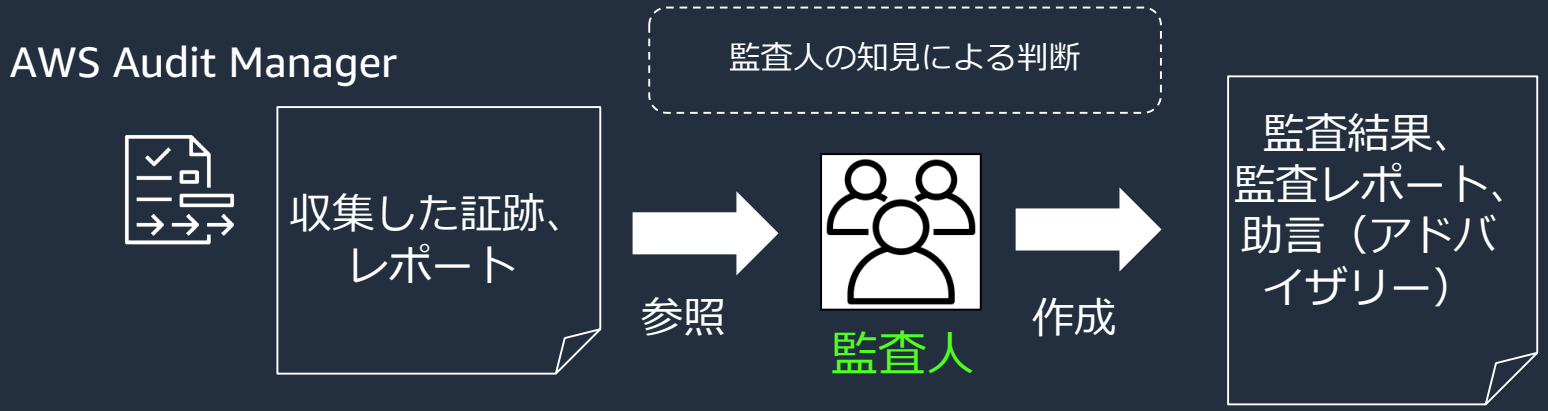
- AWS の使用状況を継続的に監査して、従来手動で行われていた証跡収集作業を削減し、AWSのプラットフォーム自体と同じくスケールする監査をサポートする
- AWS Audit Manager には CIS AWS Foundation Benchmark, GDPR, PCI DSS などの業界標準や認証が監査に要求する項目に対応するテンプレートが入っており、AWS 上の監査証跡を自動で収集します

- 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

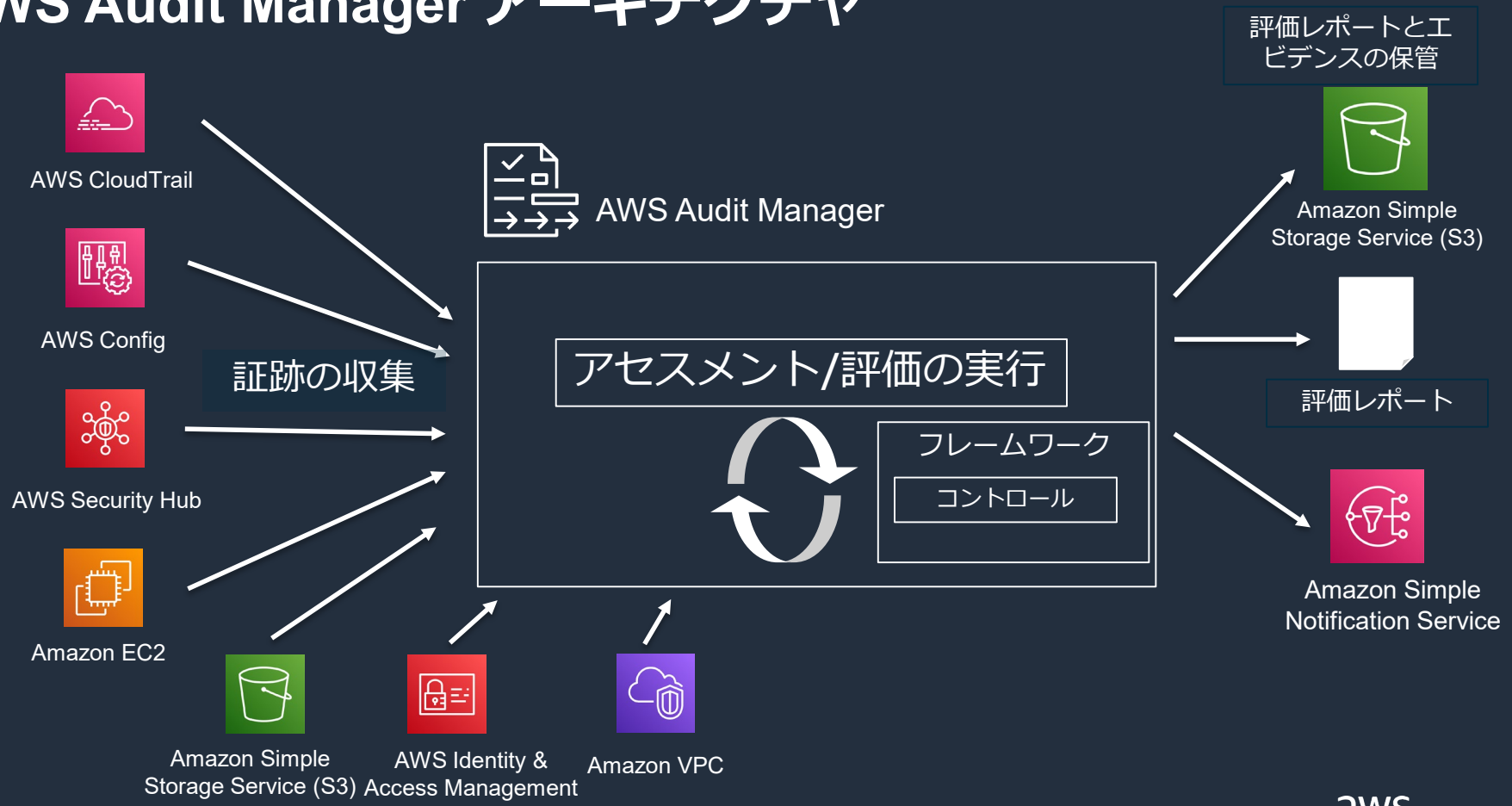
- 監査人が得るメリット
    - 監査証跡の収集を手動で行う手間の削減
    - 監査証跡の真正性が Audit Manager で担保される
    - リアルタイムに近い形で最新の証跡を取得出来る

# 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サポートのためのサービス



# 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

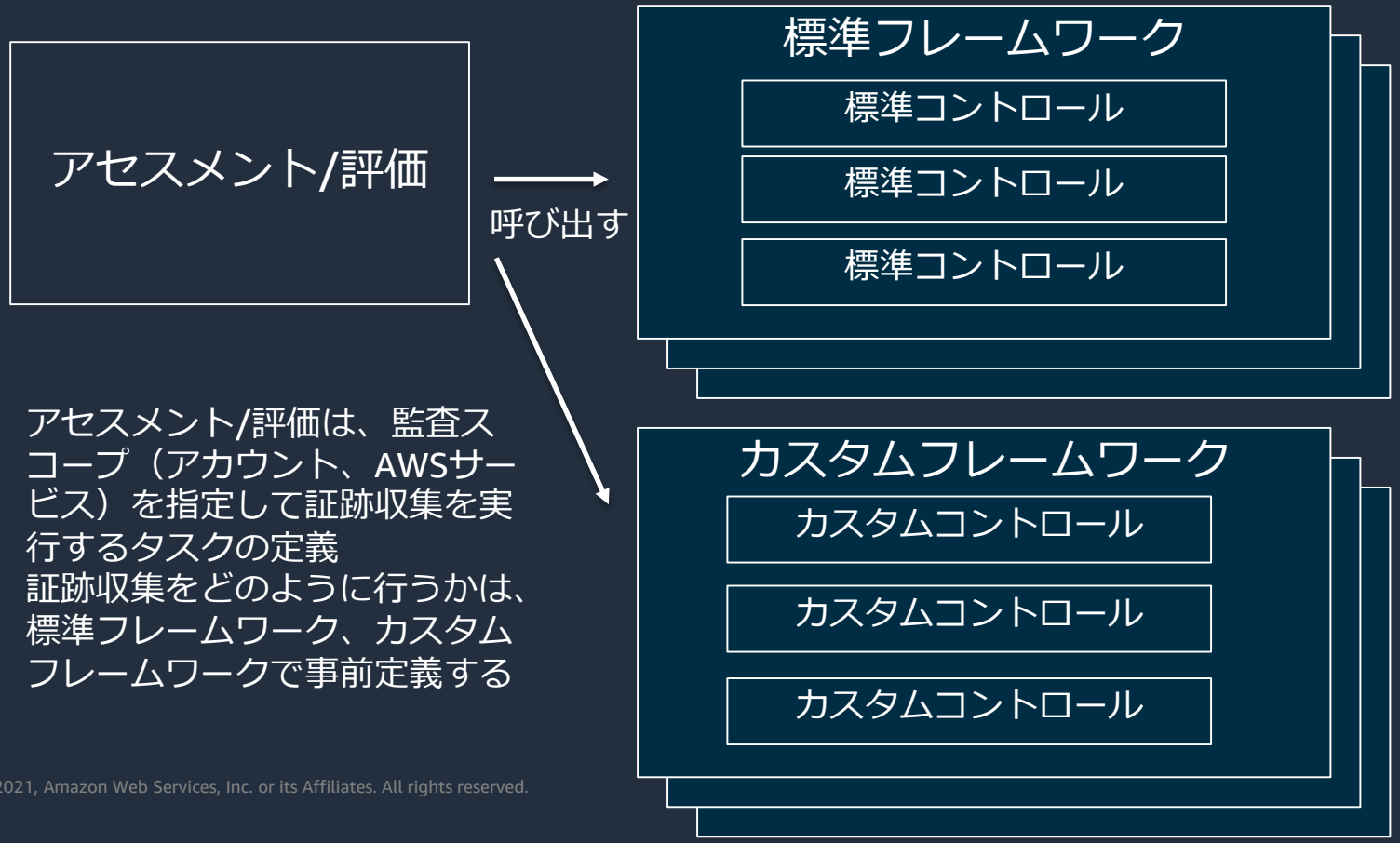
設定方法、設定例

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




- アセスメント/評価は、監査スコープ（アカウント、AWSサービス）を指定して証跡収集を実行するタスクの定義
- 証跡収集をどのように行うかは、標準フレームワーク、カスタムフレームワークで事前定義する

# 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 |

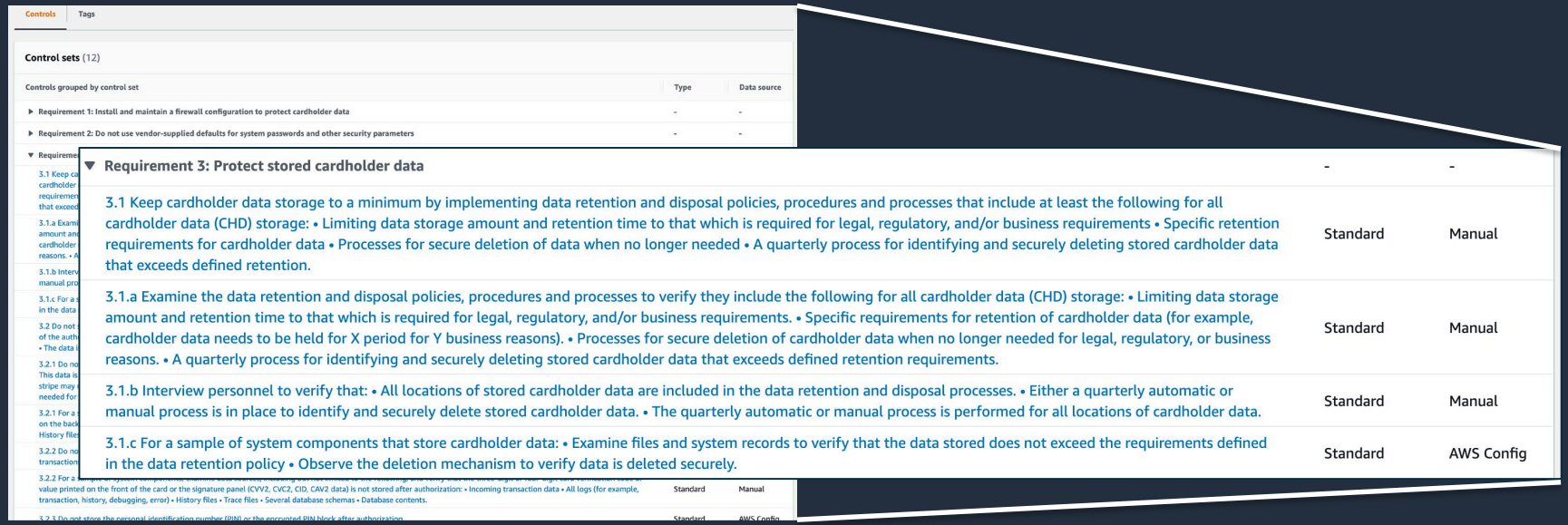
参考 https://docs.aws.amazon.com/ja_jp/audit-manager/latest/userguide/framework-overviews.html

# Audit Manager が提供するフレームワーク 2

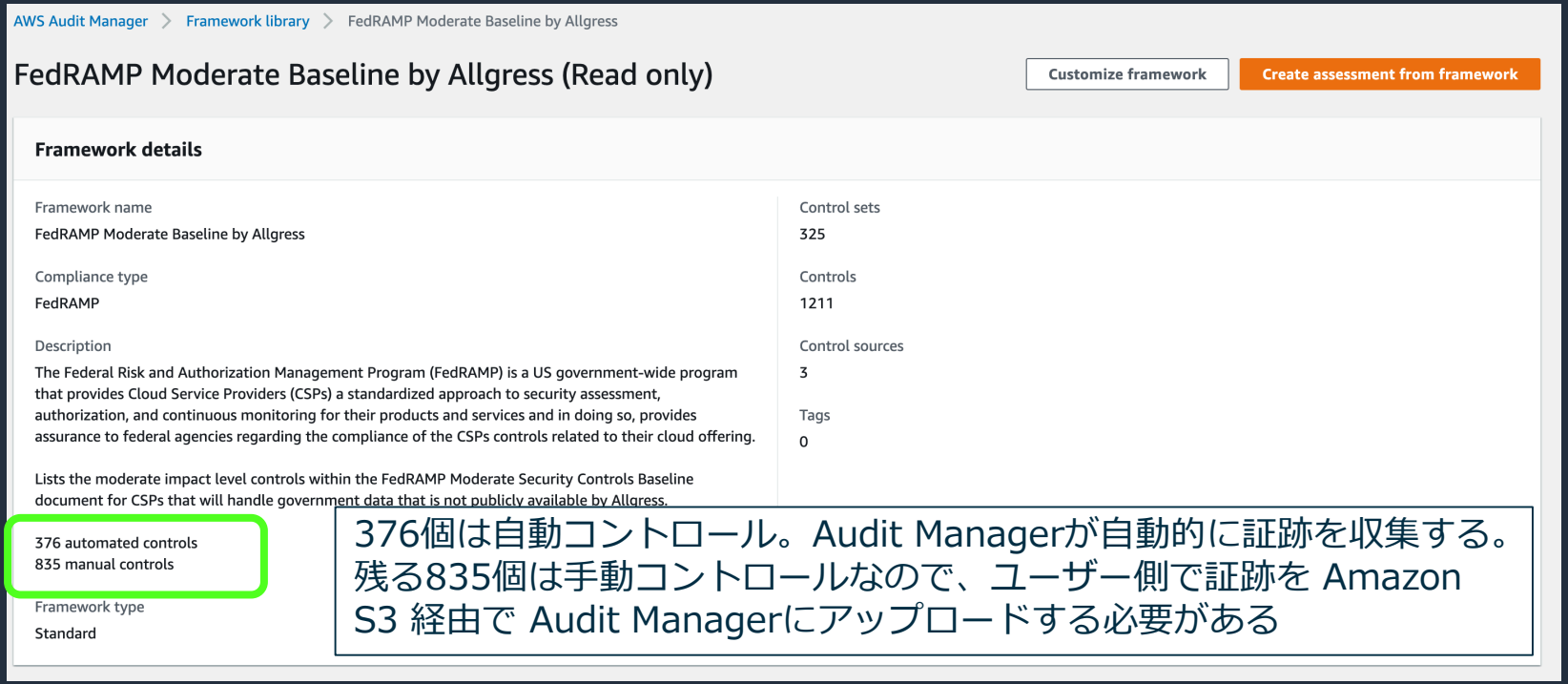
| 名称 | 説明 | 含まれる自動コントロールの数 |
|---|---|---|
| FedRAMP Allgress による中程度のベースライン | 米国政府が展開しているクラウドサービス・プロバイダーのセキュリティ評価のチェック項目を監査する | 376 |
| GDPR | EU/EEAの個人情報保護に関するレギュレーションのチェック項目 | 0 （手動コントロールは376） |
| GxP 21 CFR part 11 | 消費者に対して食料と医薬品の安全を守るために生産時のデータ整合性を保証するレギュレーション | 14 |
| HIPAA | 米国の個人健康保険情報を保護する連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



# 自動コントロールと手動コントロール



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

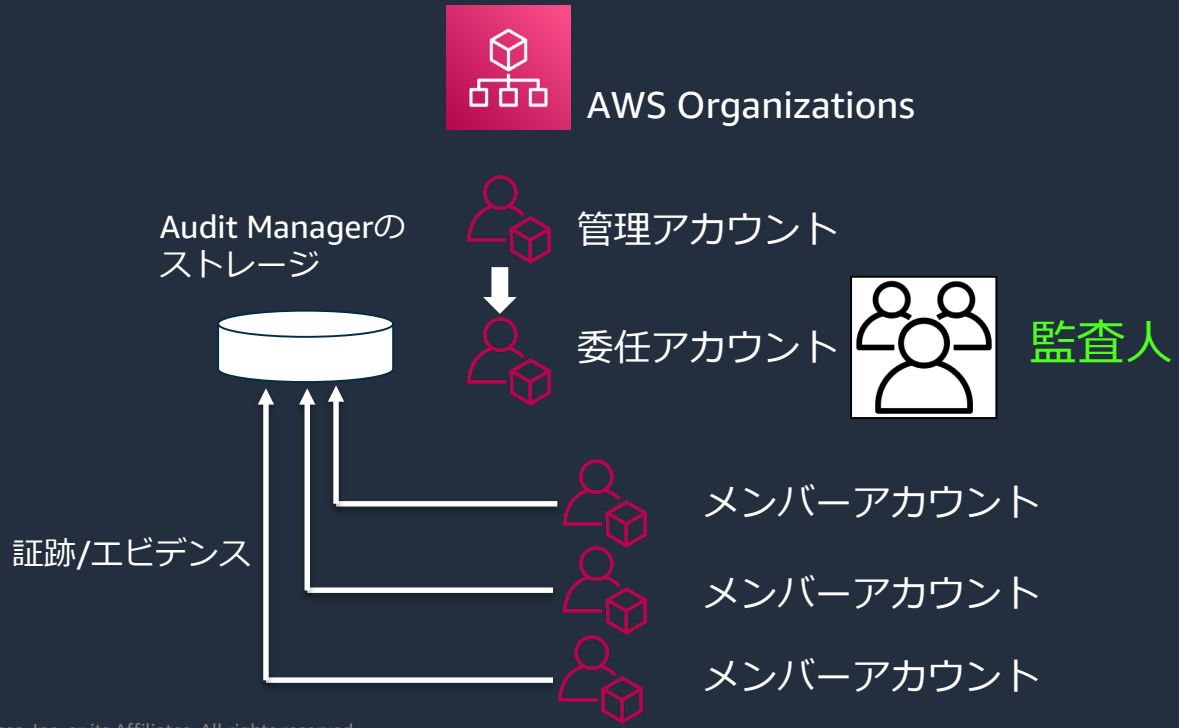
# マルチアカウント環境 の AWS Audit Manager

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

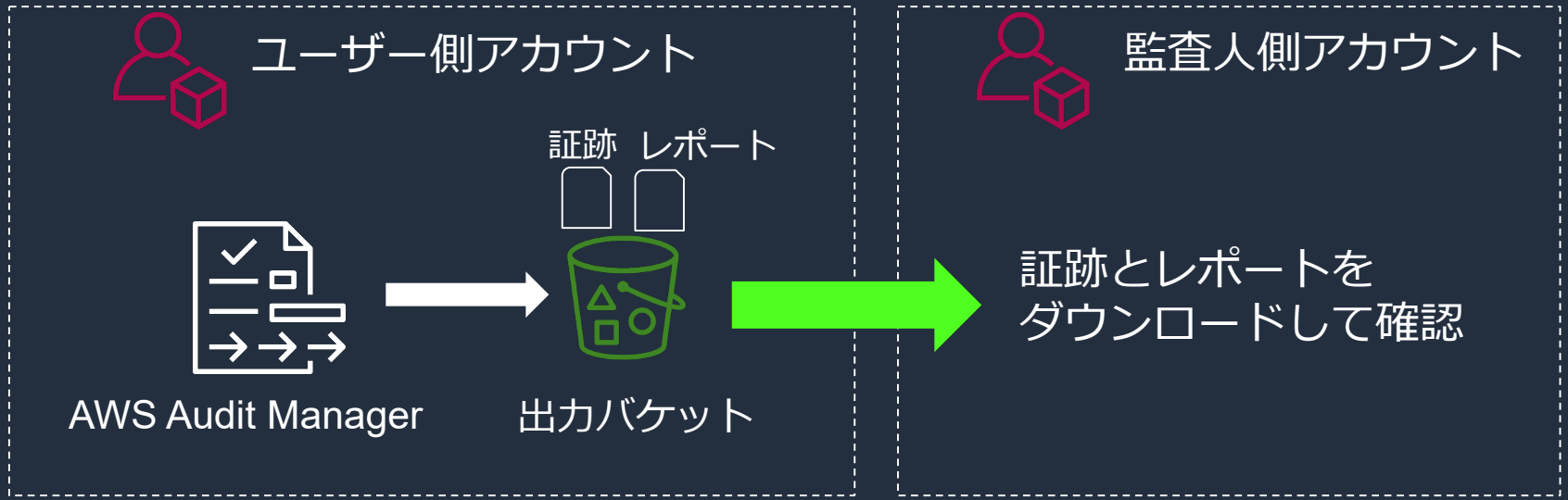
# 外部監査人が監査する場合のアーキテクチャ パターン 1

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

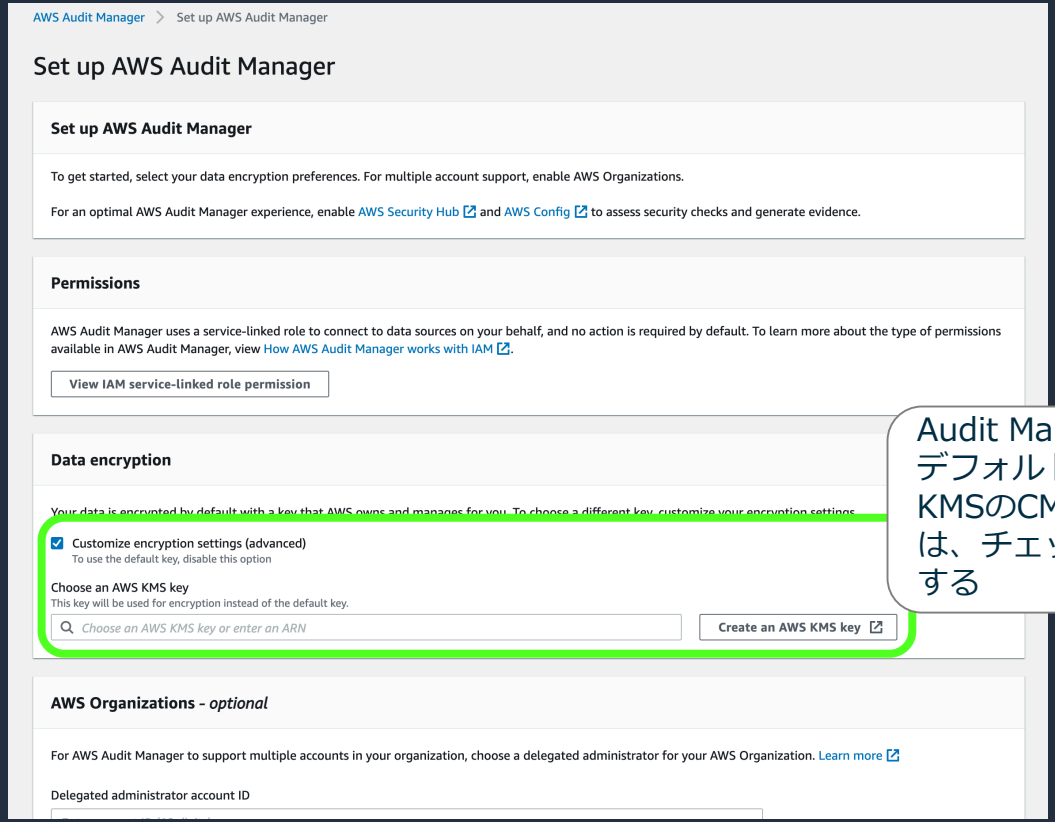
設定方法、設定例

セキュリティ、料金、制約

パートナー様との協業

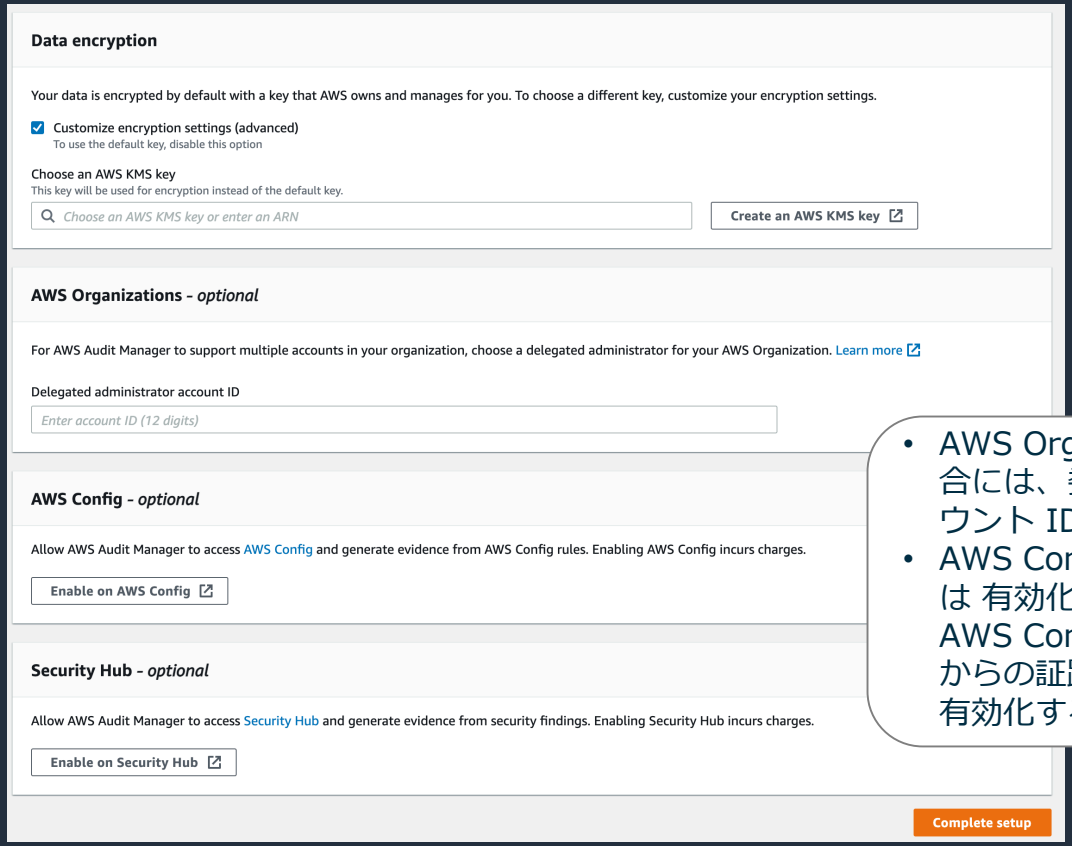
まとめ

# Audit Manager の初期セットアップ 1



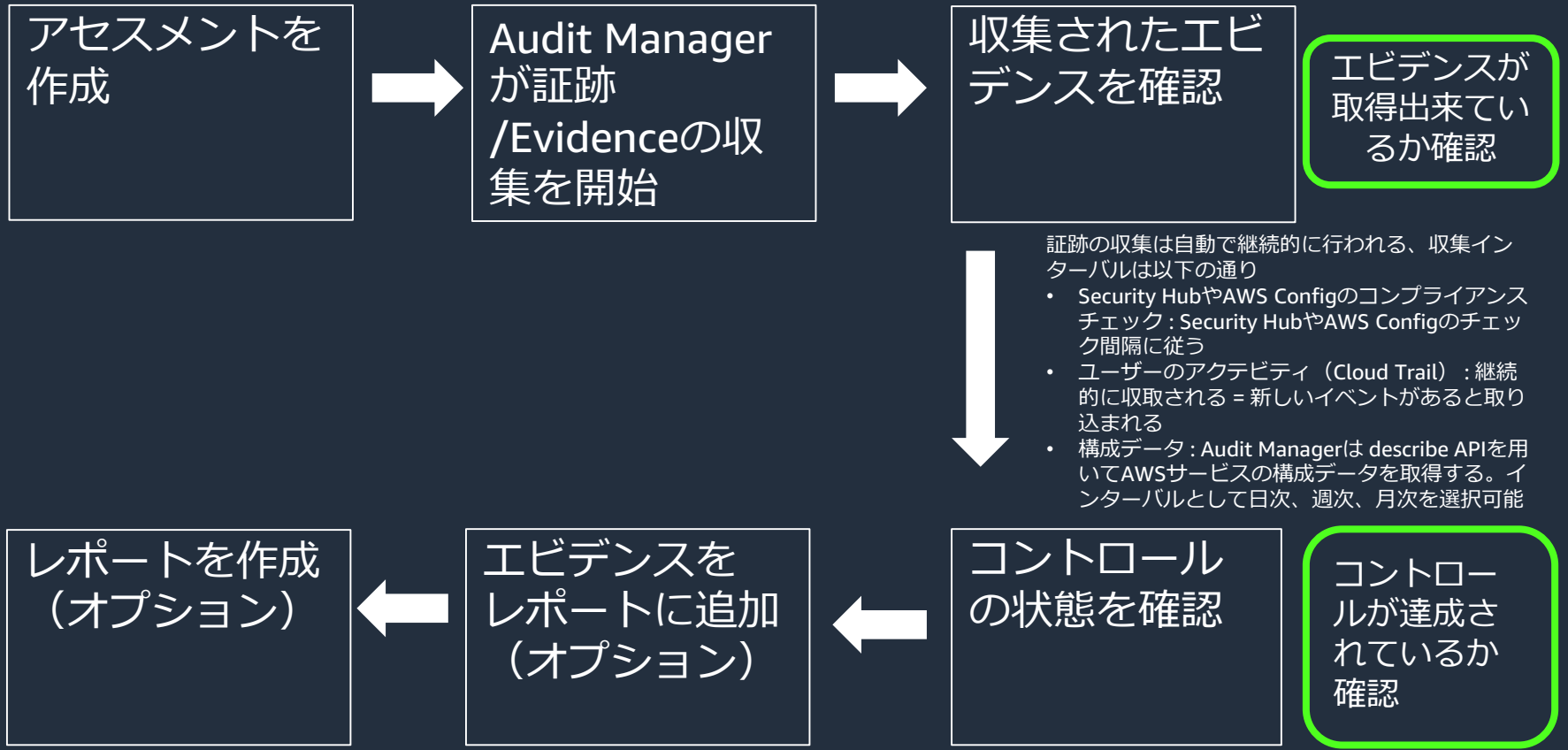

Audit Managerのデータは
デフォルトで暗号化されるが、
KMSのCMKで暗号化したい場合には、チェックをして、CMKを指定する

# Audit Manager の初期セットアップ 2

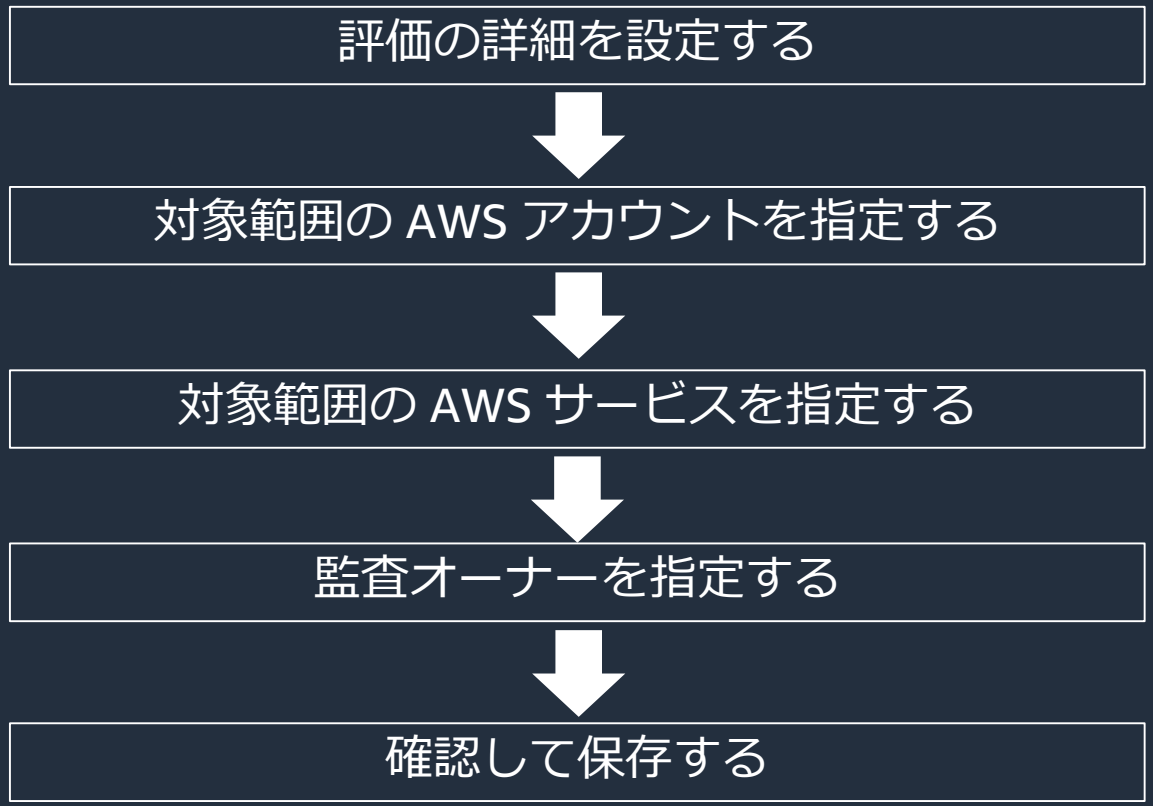



- AWS Organizations 環境の場合には、委任する管理者のアカウント ID を指定する
- AWS Config や Security Hub は 有効化されていないと、AWS Config や Security Hub からの証跡収集が出来ないので、有効化することが推奨

# Audit Manager 評価の実行と、レポート作成までの流れ

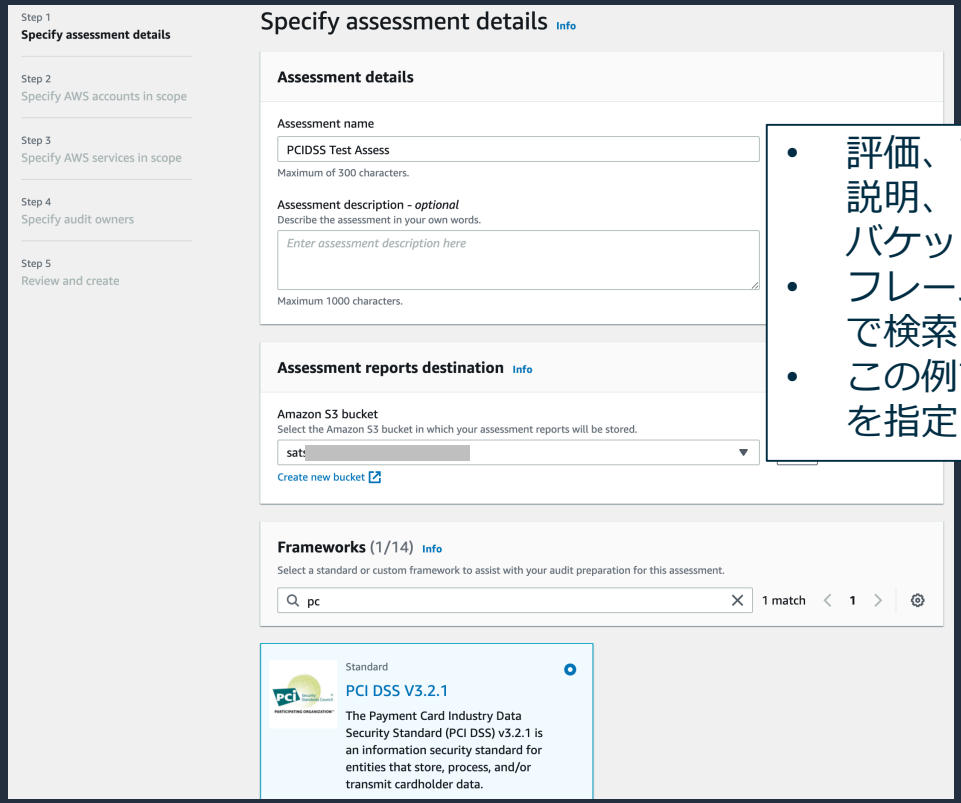


# 評価/アセスメントの作成手順



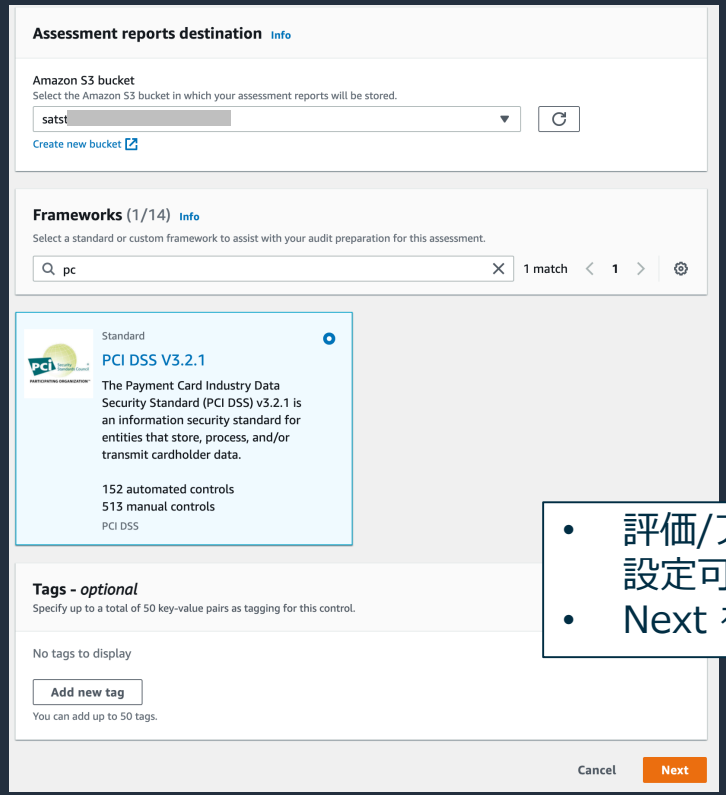

参考：https://docs.aws.amazon.com/ja_jp/audit-manager/latest/userguide/create-assessments.html

# 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




- 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

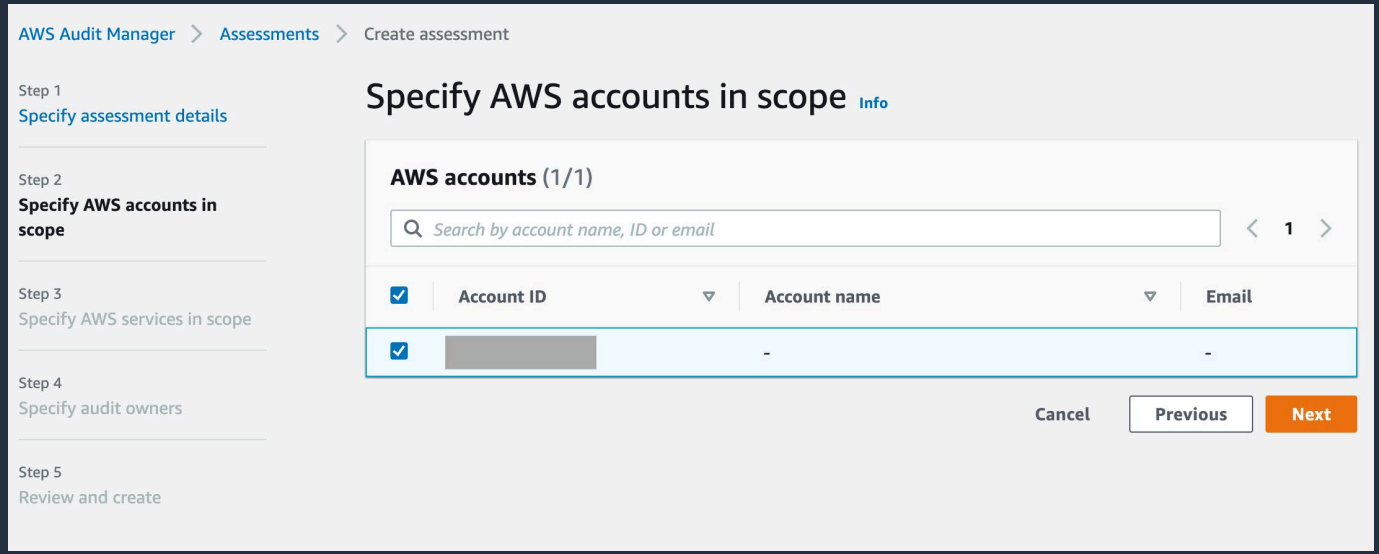
# Audit Manager が提供するフレームワークを使った評価/アセスメントの作成手順 2



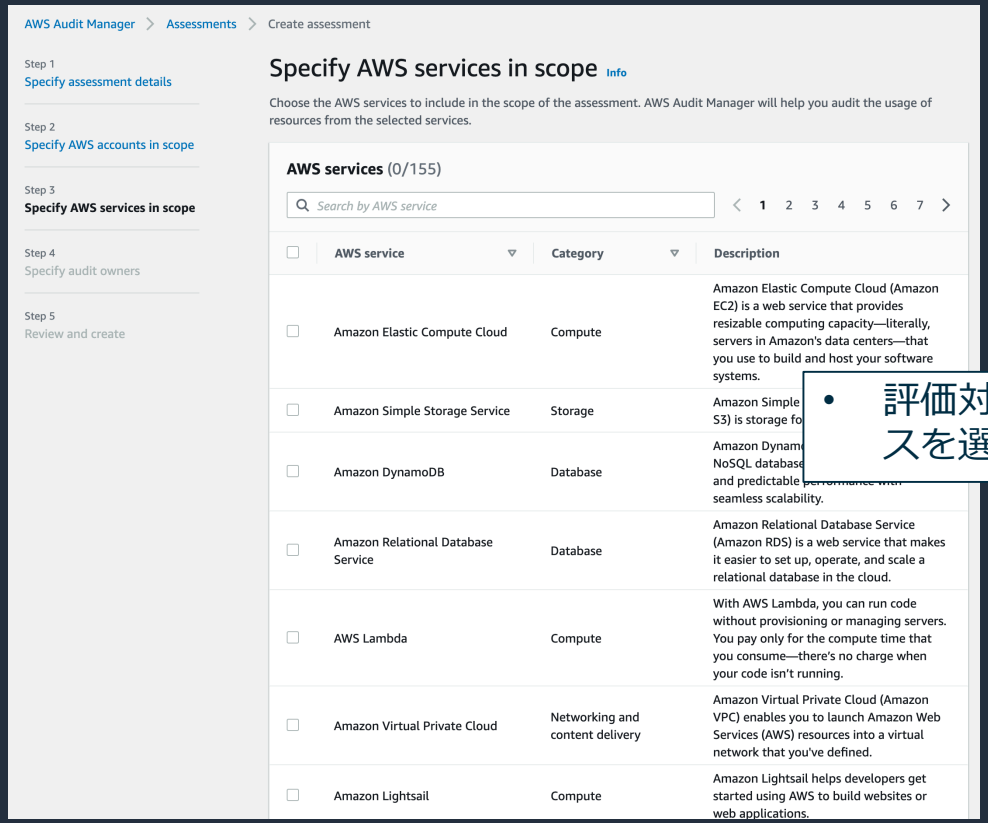

- 評価/アセスメントに任意のタグを設定可能
- Next を押して次のステップに進む

# 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

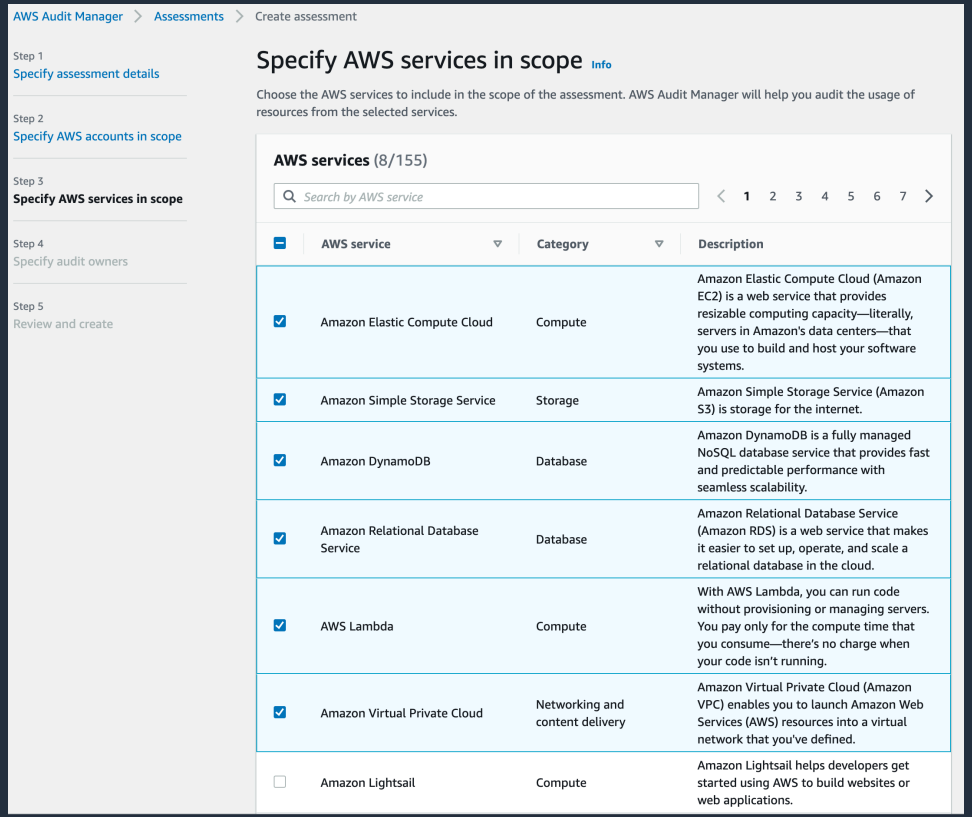


# Audit Manager が提供するフレームワークを使った評価/アセスメントの作成手順 4

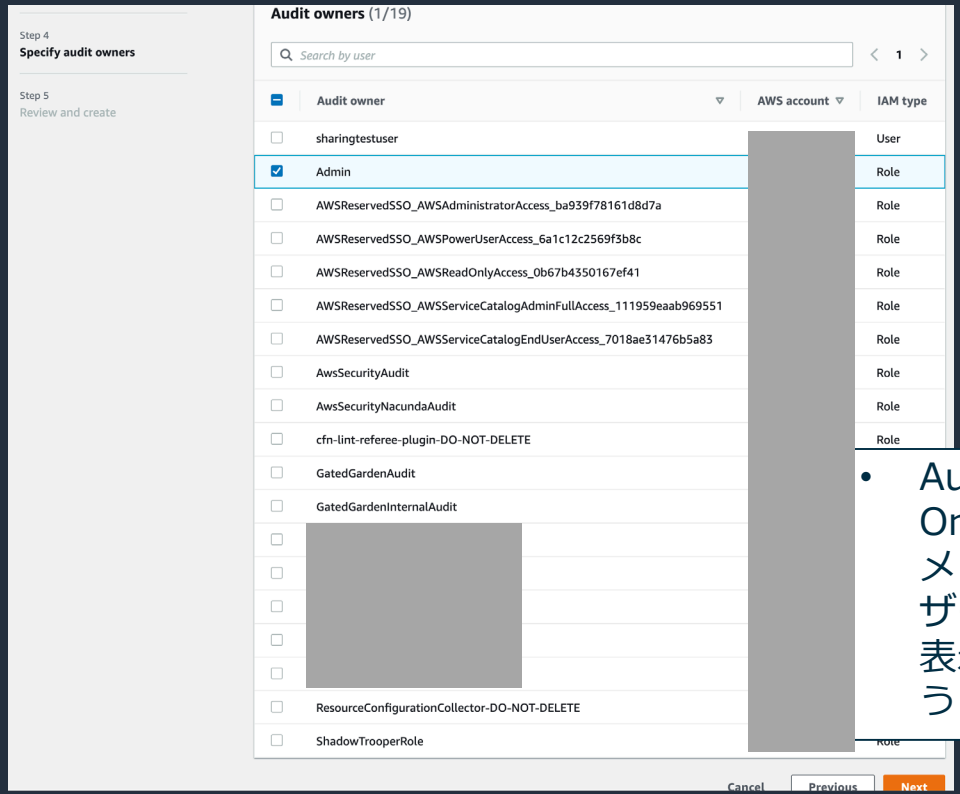



- 評価対象とする、AWS サービスを選択する

# 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

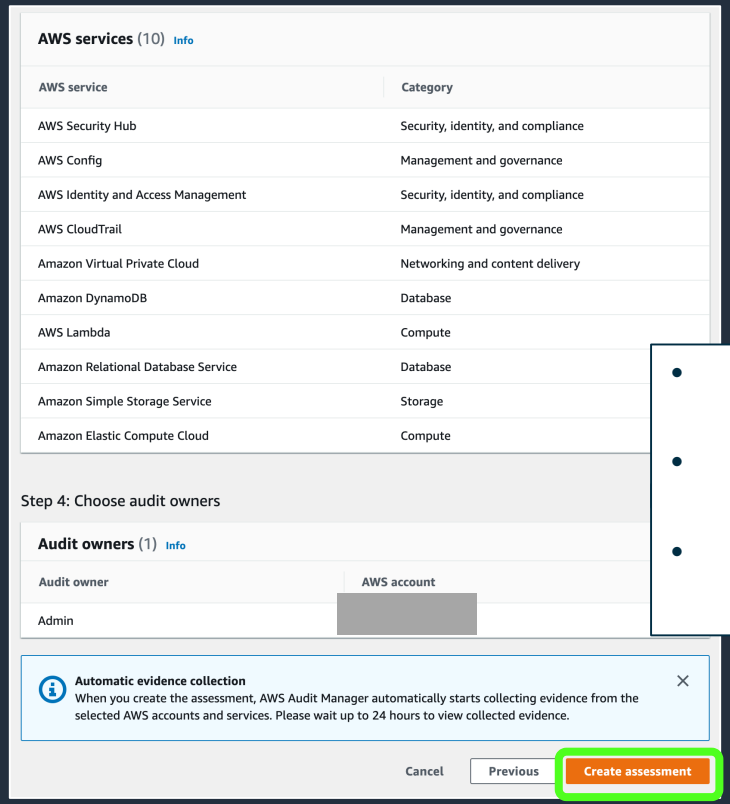


# Audit Manager が提供するフレームワークを使った評価/アセスメントの作成手順 6




- 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

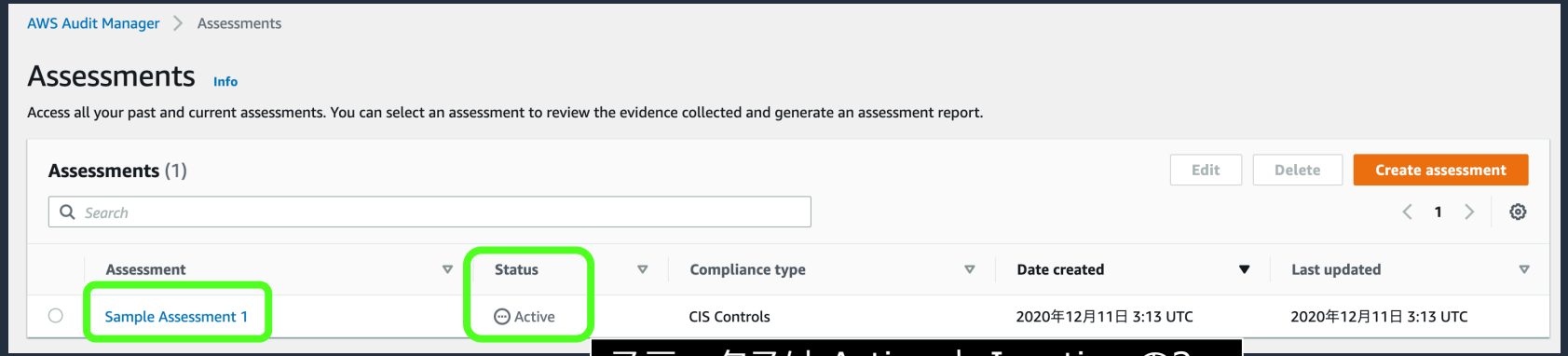
# Audit Manager が提供するフレームワークを使った評価/アセスメントの作成手順 7




- 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

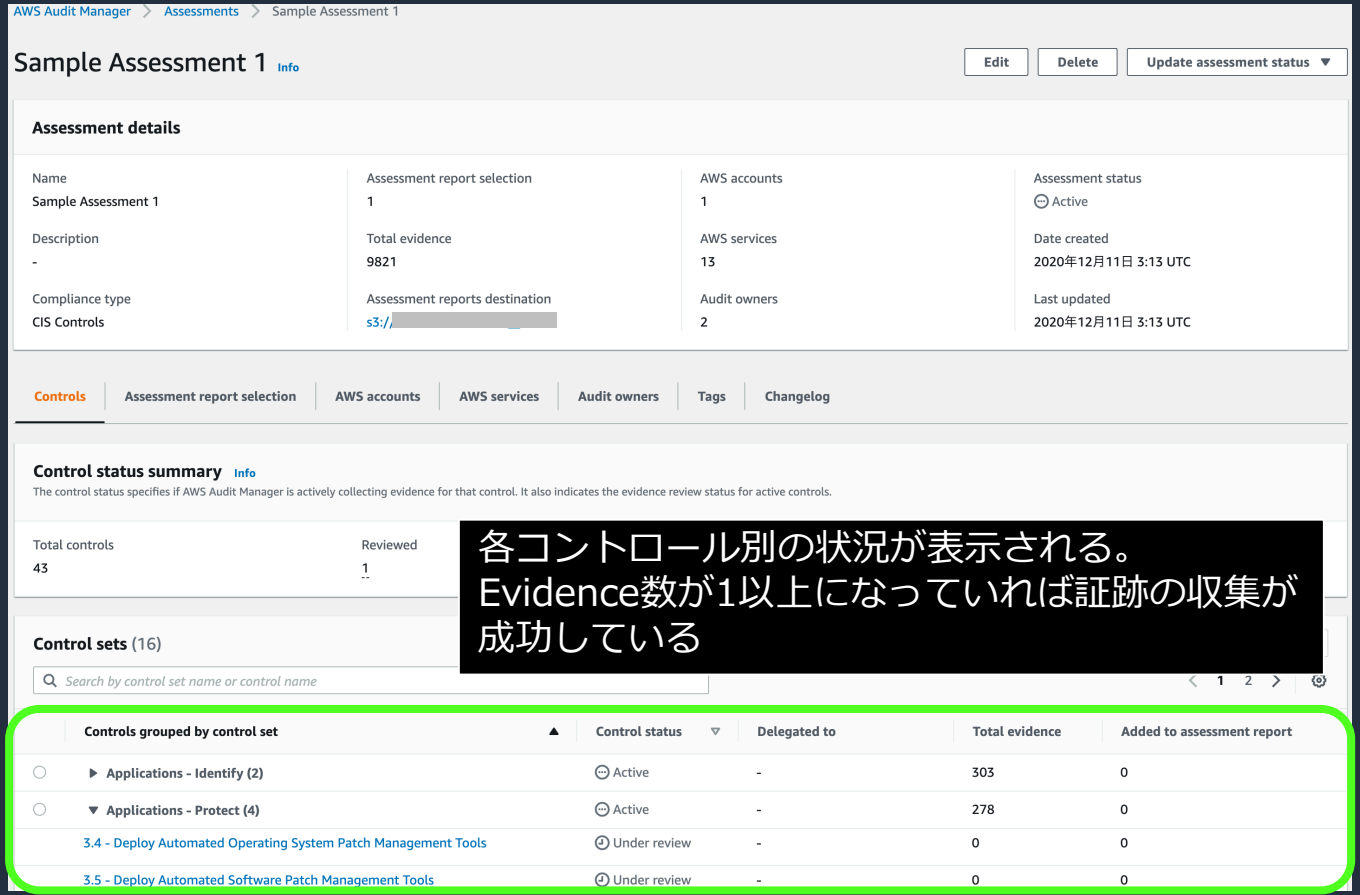
- 評価/アセスメントを作成して最初の結果が出るまでは、フレームワークの項目数などにも依存しますが、最大24時間程度かかります
- 実行している評価/アセスメントのステータスを確認することが可能です
- マネージメントコンソール の Assessments を選択すると、現在作成されている評価/アセスメントの一覧が表示される



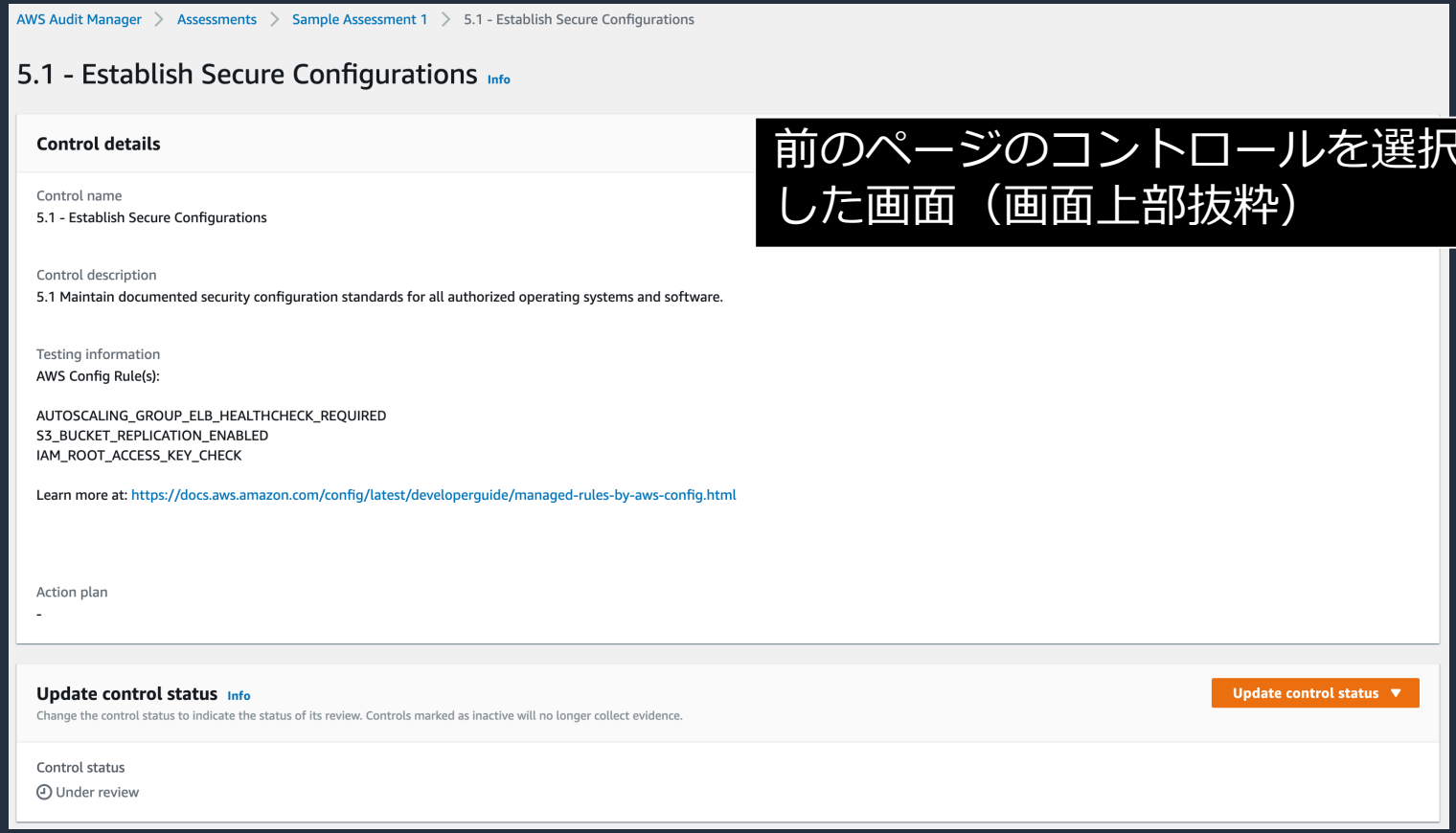

アセスメント名を選択すると詳細な状況が表示される

ステータスは Active と Inactive の2種類、Active は証跡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

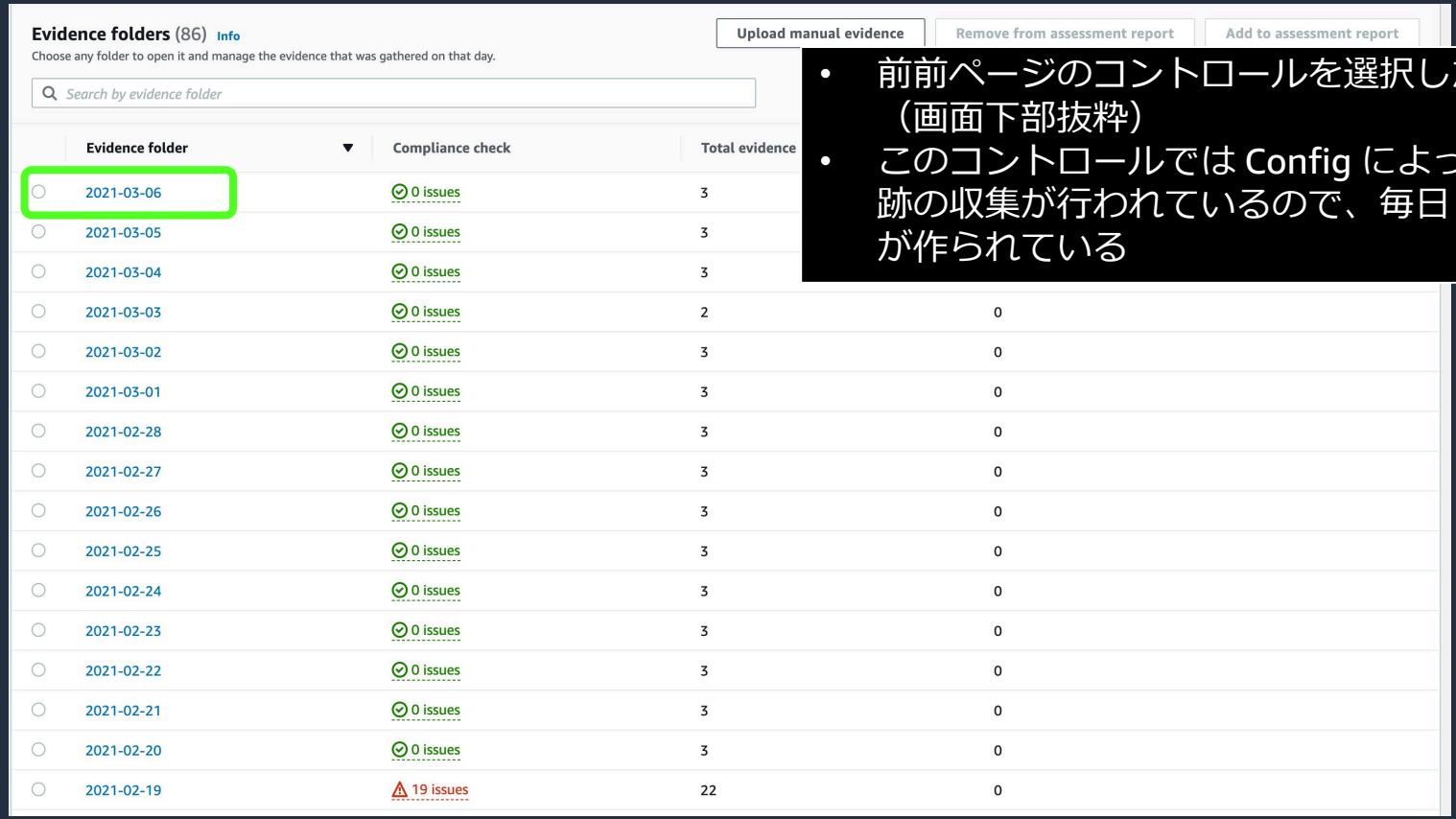


# 評価/アセスメントのステータスの確認 3



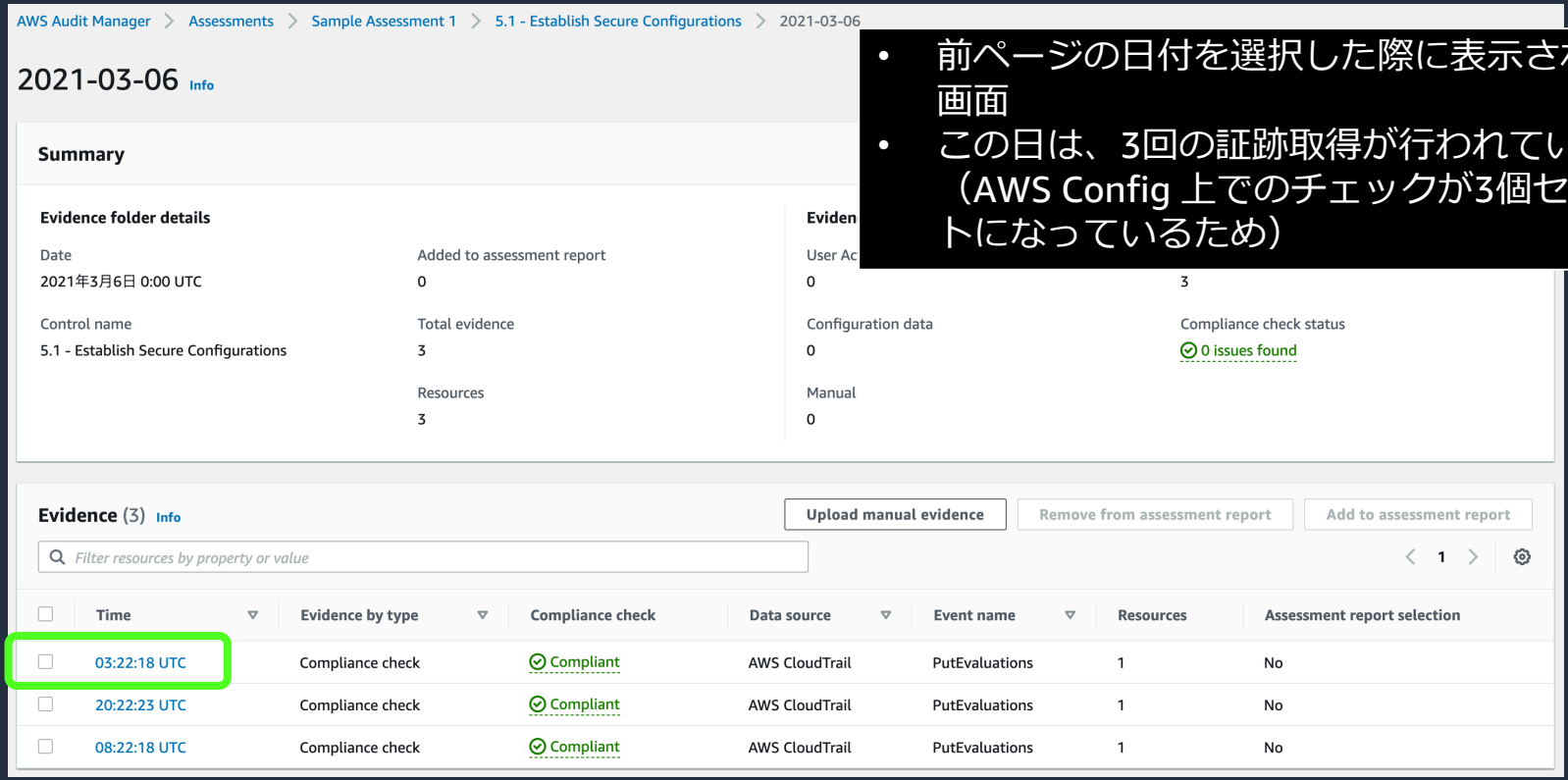

前のページのコントロールを選択した画面（画面上部抜粋）

# 評価/アセスメントのステータスの確認 4



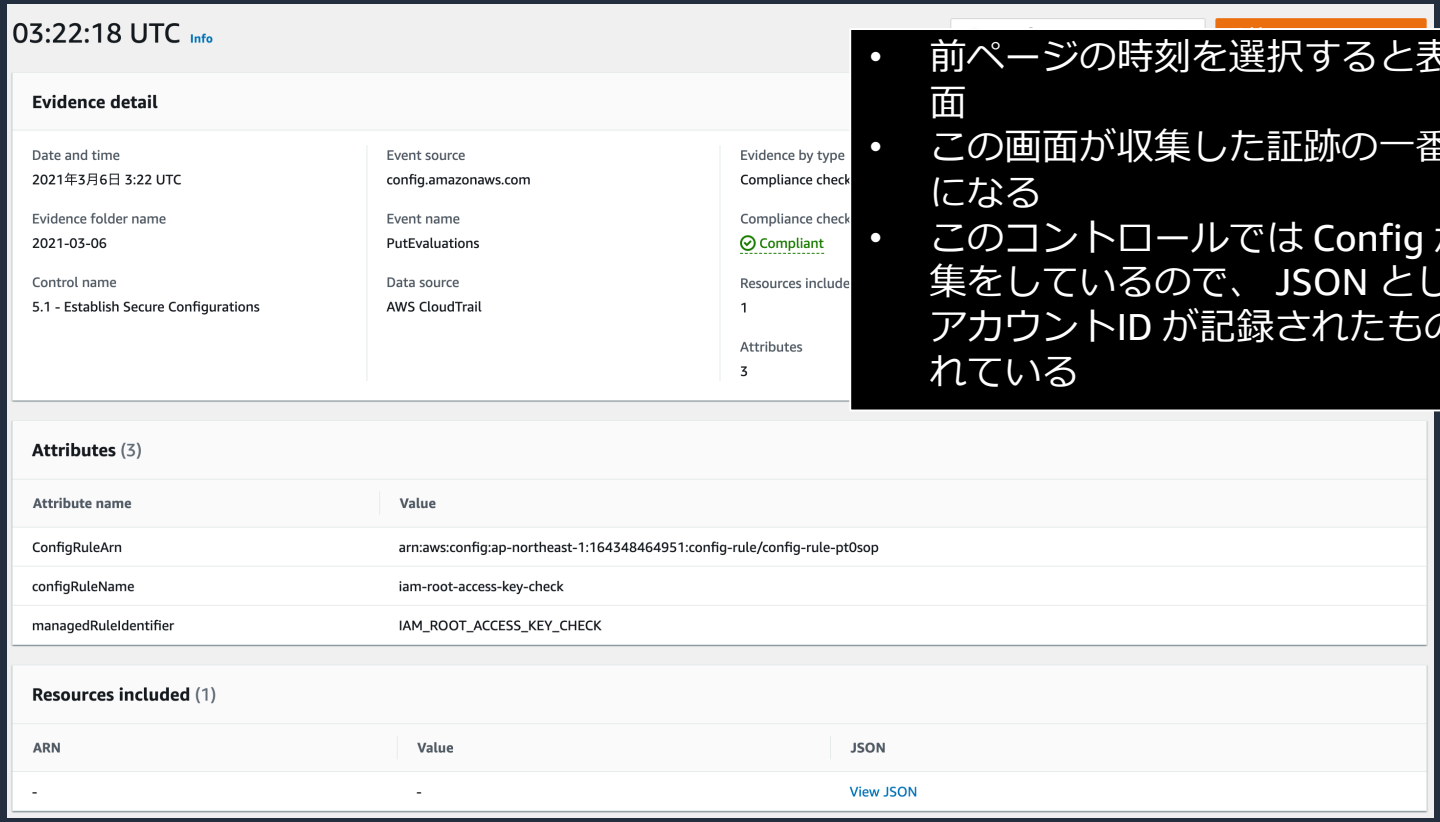

- 前前ページのコントロールを選択した画面（画面下部抜粋）
- このコントロールでは Config によって証跡の収集が行われているので、毎日 証跡が作られている

# 評価/アセスメントのステータスの確認 5



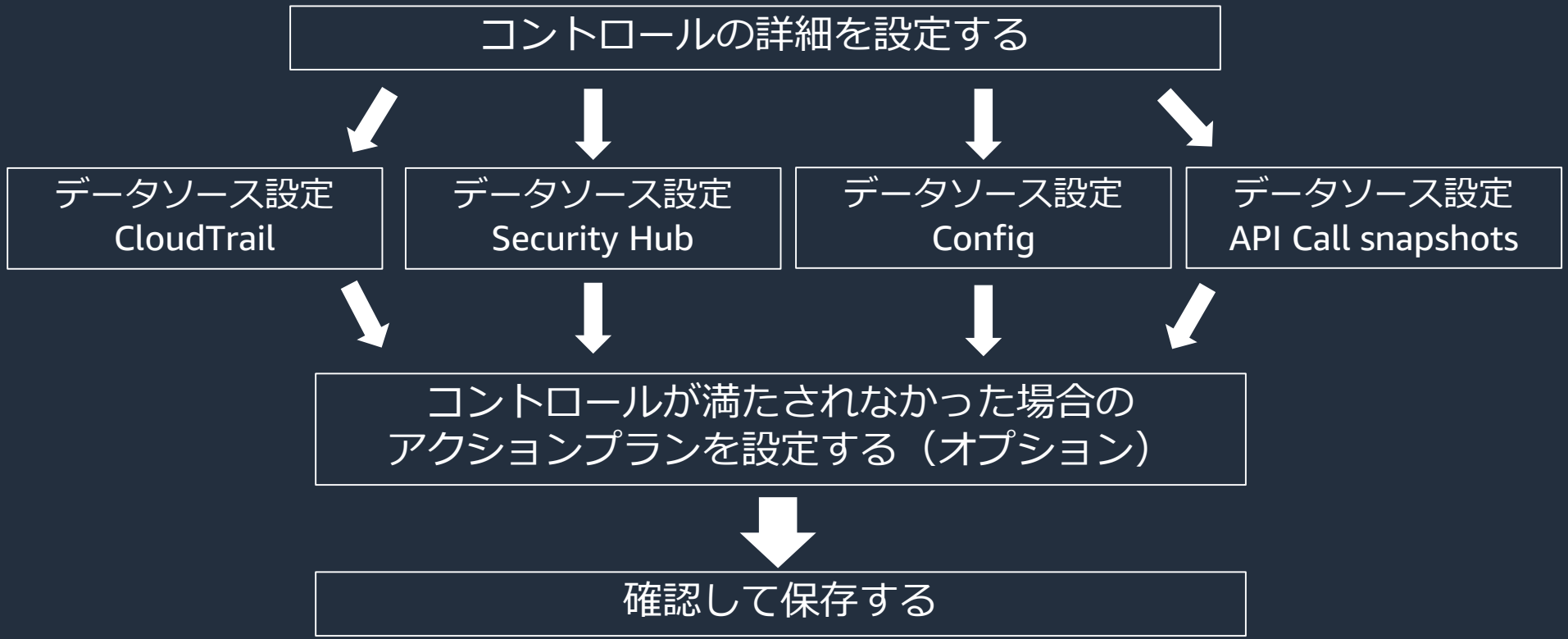

- 前ページの日付を選択した際に表示される画面
- この日は、3回の証跡取得が行われている（AWS Config 上でのチェックが3個セットになっているため）

# 評価/アセスメントのステータスの確認 5



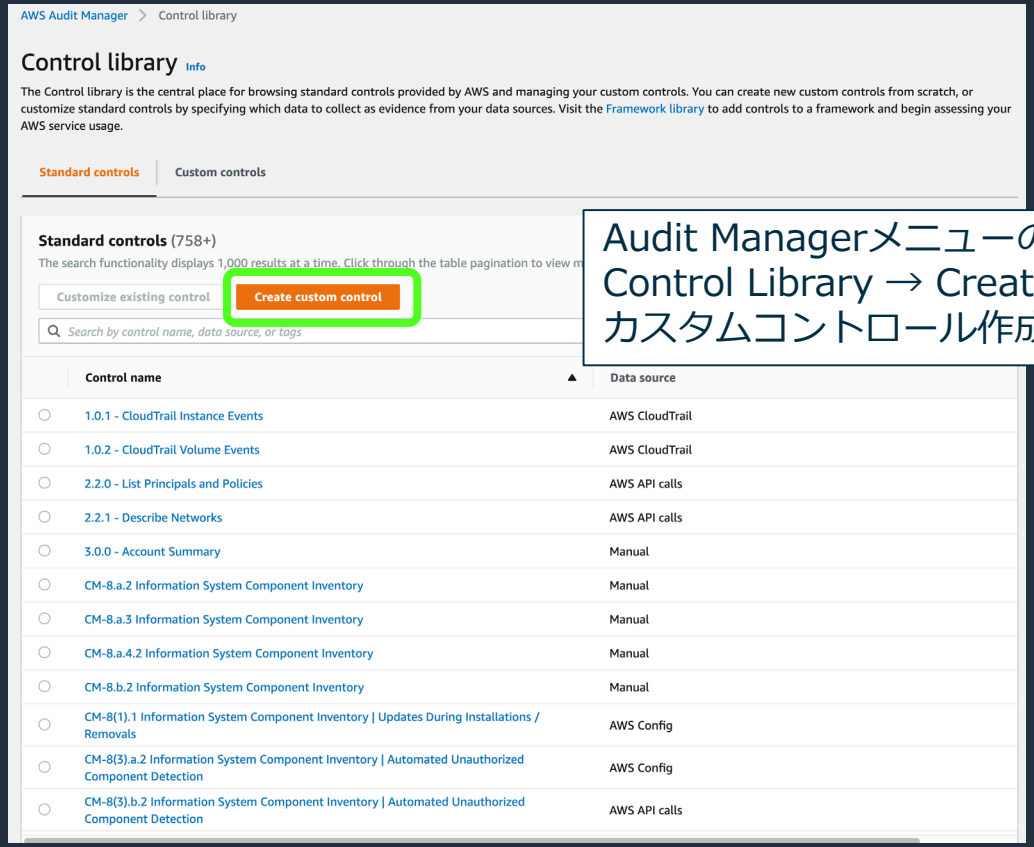

- 前ページの時刻を選択すると表示される画面
- この画面が収集した証跡の一番詳細な画面になる
- このコントロールでは Config がデータ収集をしているので、 JSON として収集したアカウントID が記録されたものが添付されている

# カスタムコントロールの作成手順



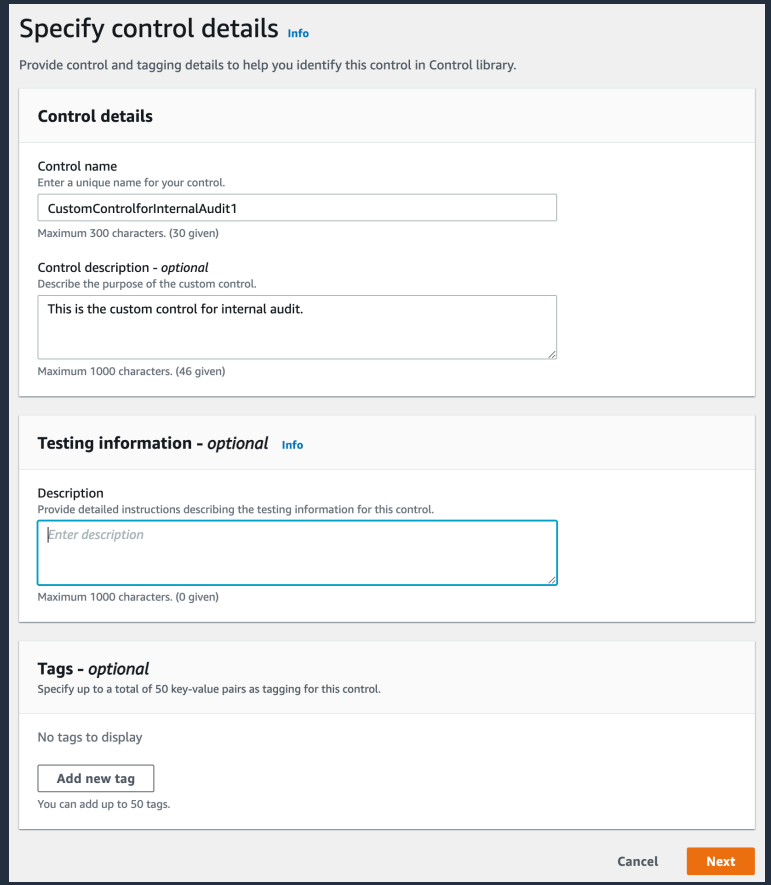

参照 : https://docs.aws.amazon.com/ja_jp/audit-manager/latest/userguide/customize-control-from-scratch.html

# カスタムコントロールの作成 1



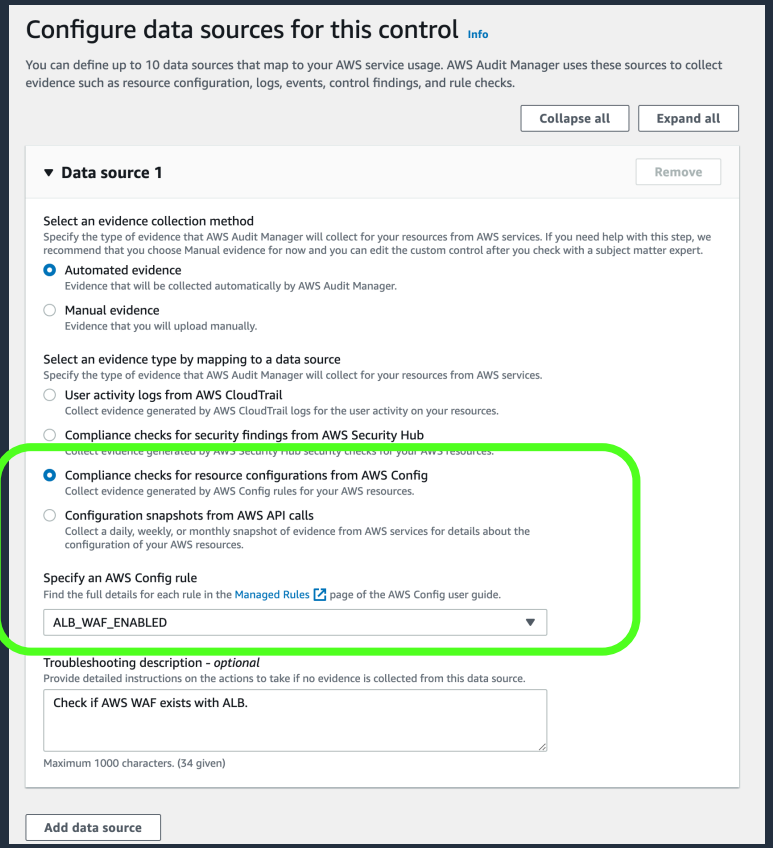

Audit Managerメニューの
Control Library → Create Custom Control で
カスタムコントロール作成画面に入る

# カスタムコントロールの作成 2



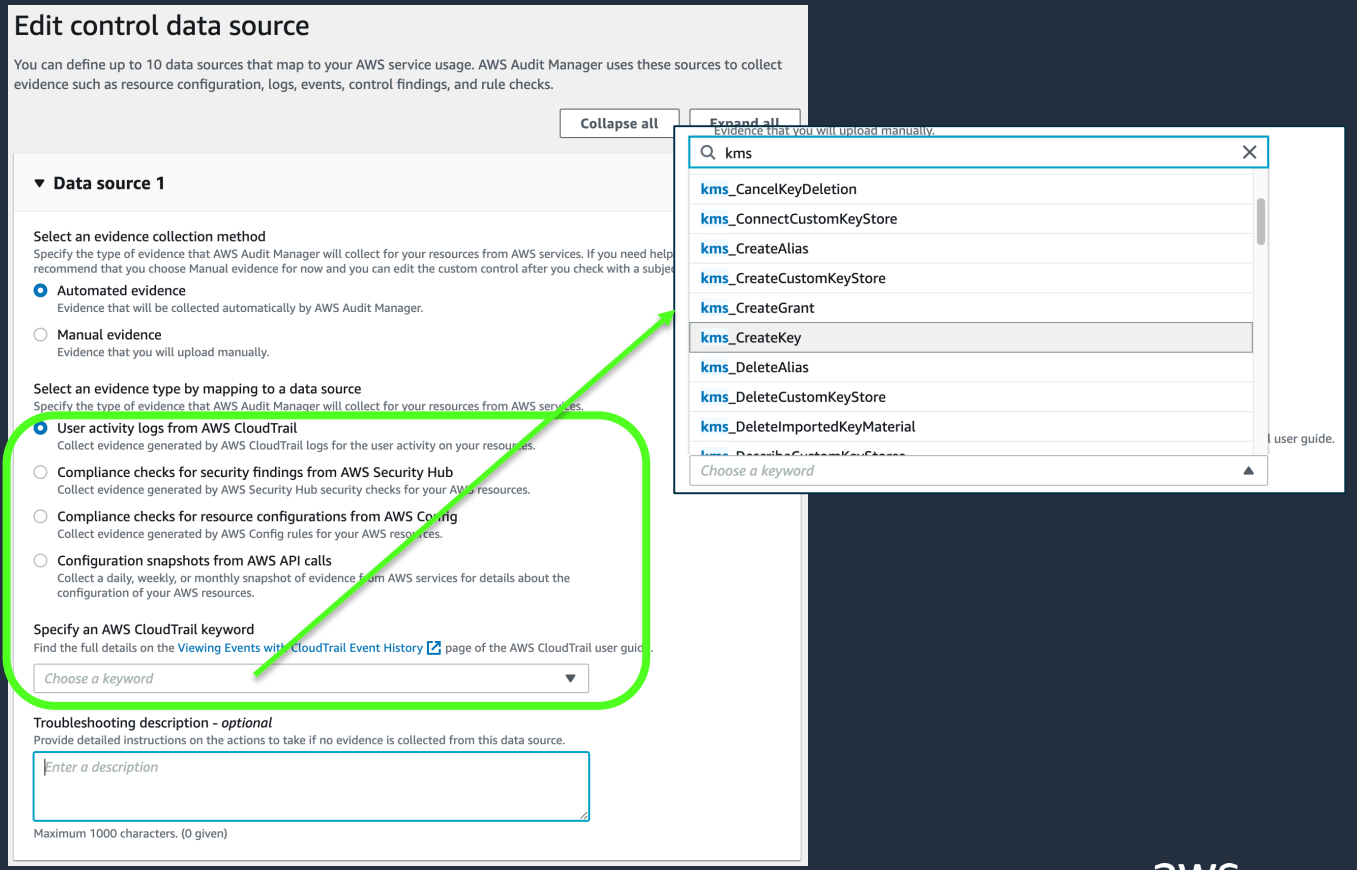
# カスタムコントロールの作成 3

- 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



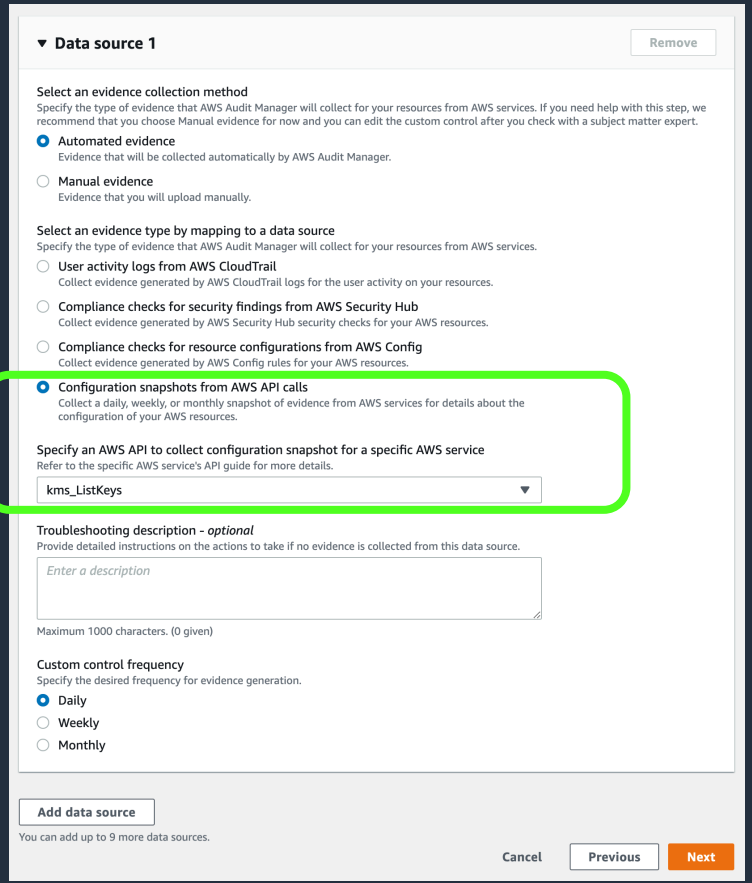
# カスタムコントロールの作成 4

- 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



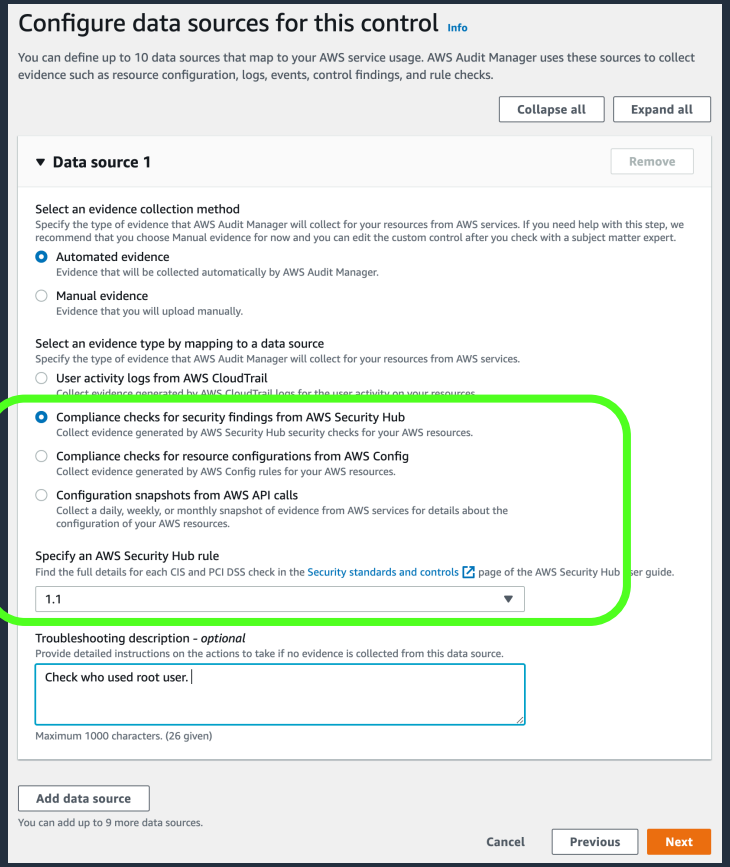
# カスタムコントロールの作成 5

- 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みの 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



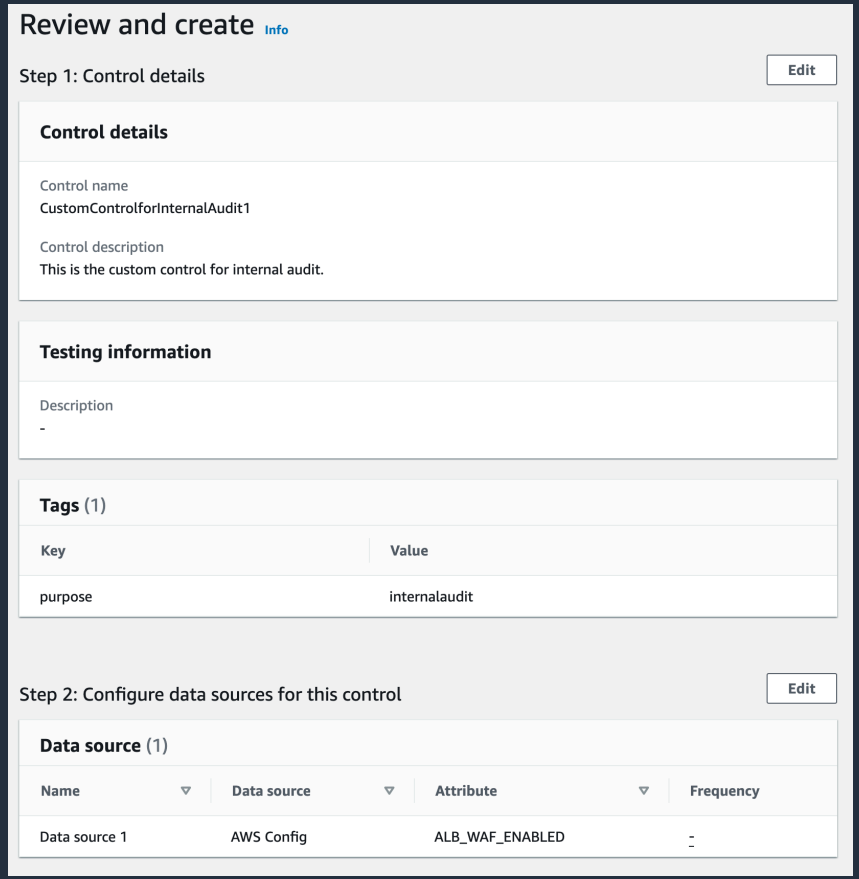
# カスタムコントロールの作成 6

- 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



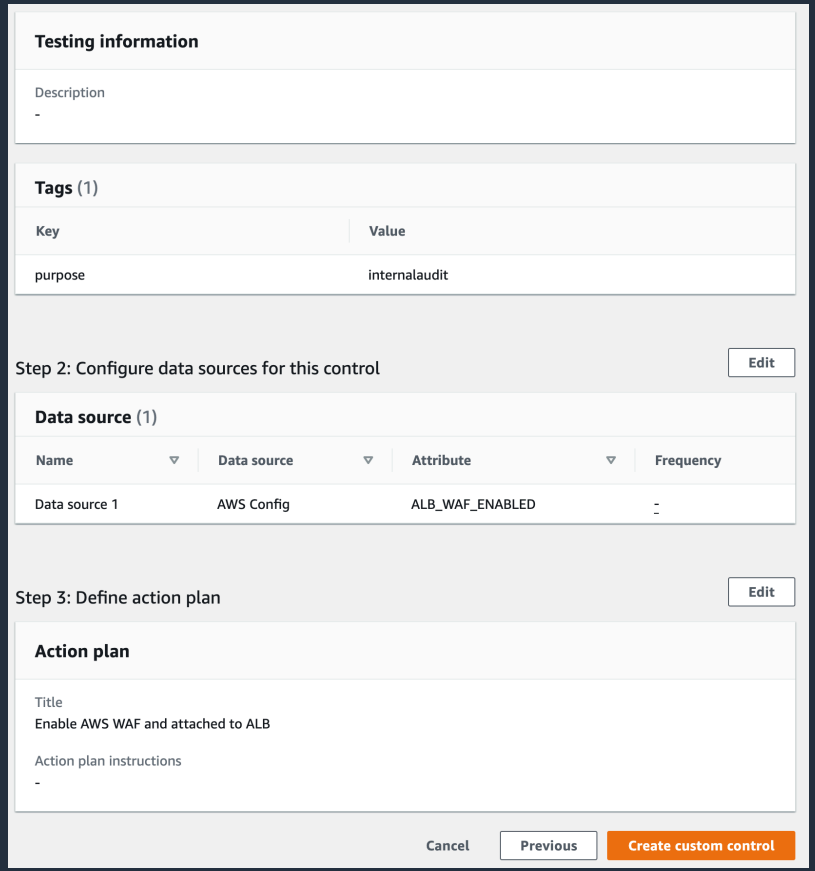
# カスタムコントロールの作成 7

- 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

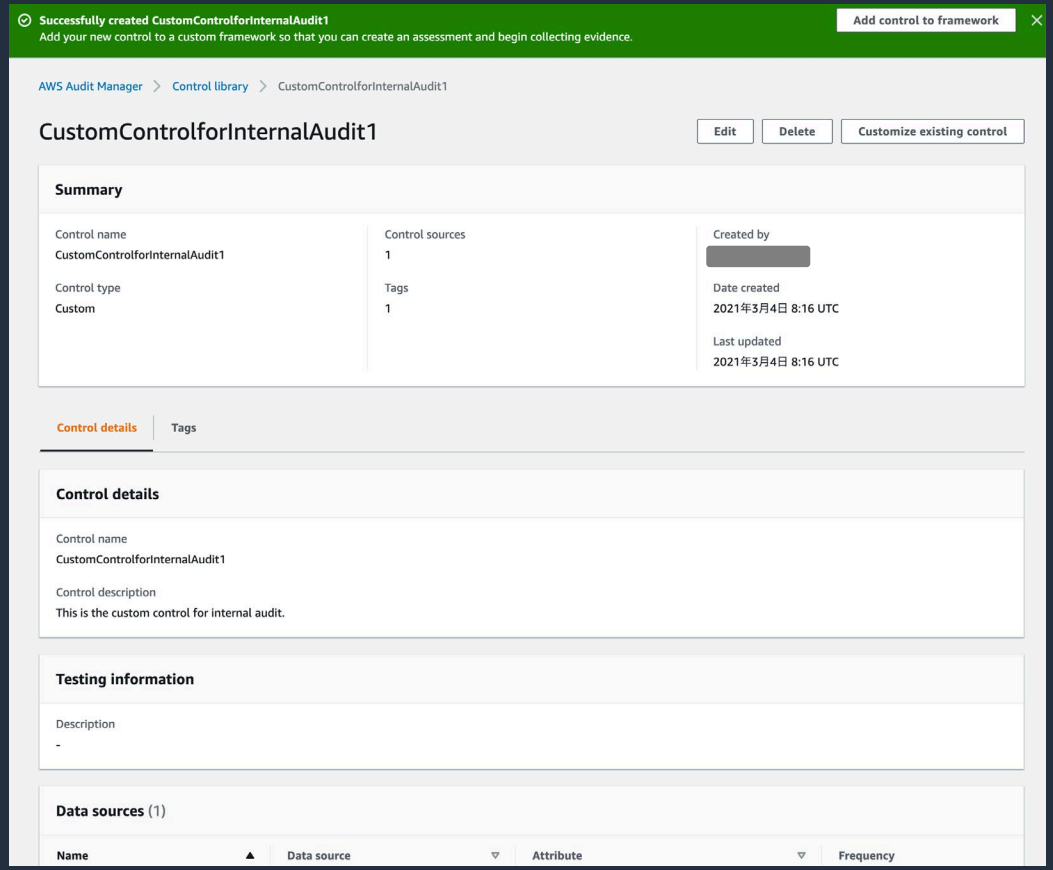


# カスタムコントロールの作成 8

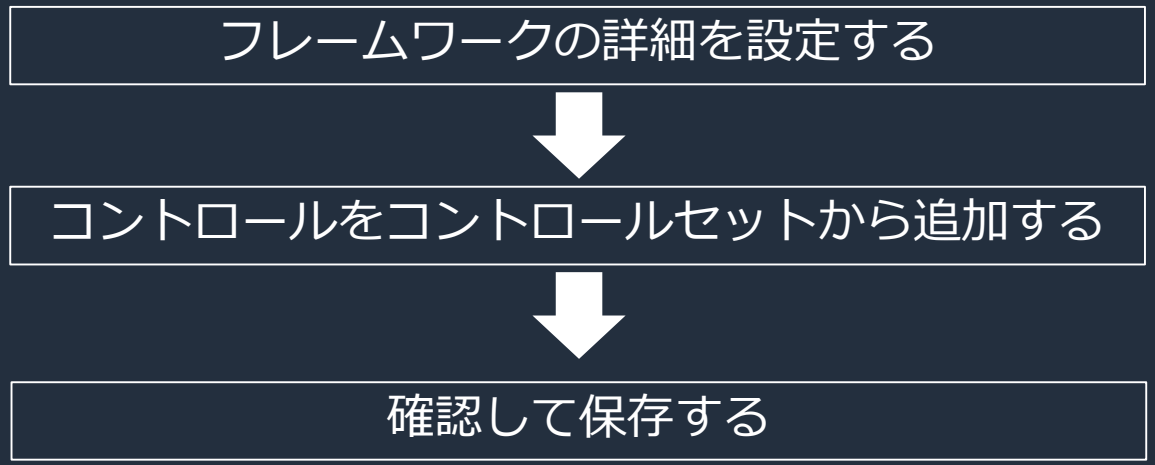
- 内容を確認して、Create custom control ボタンを押すと作成が完了する



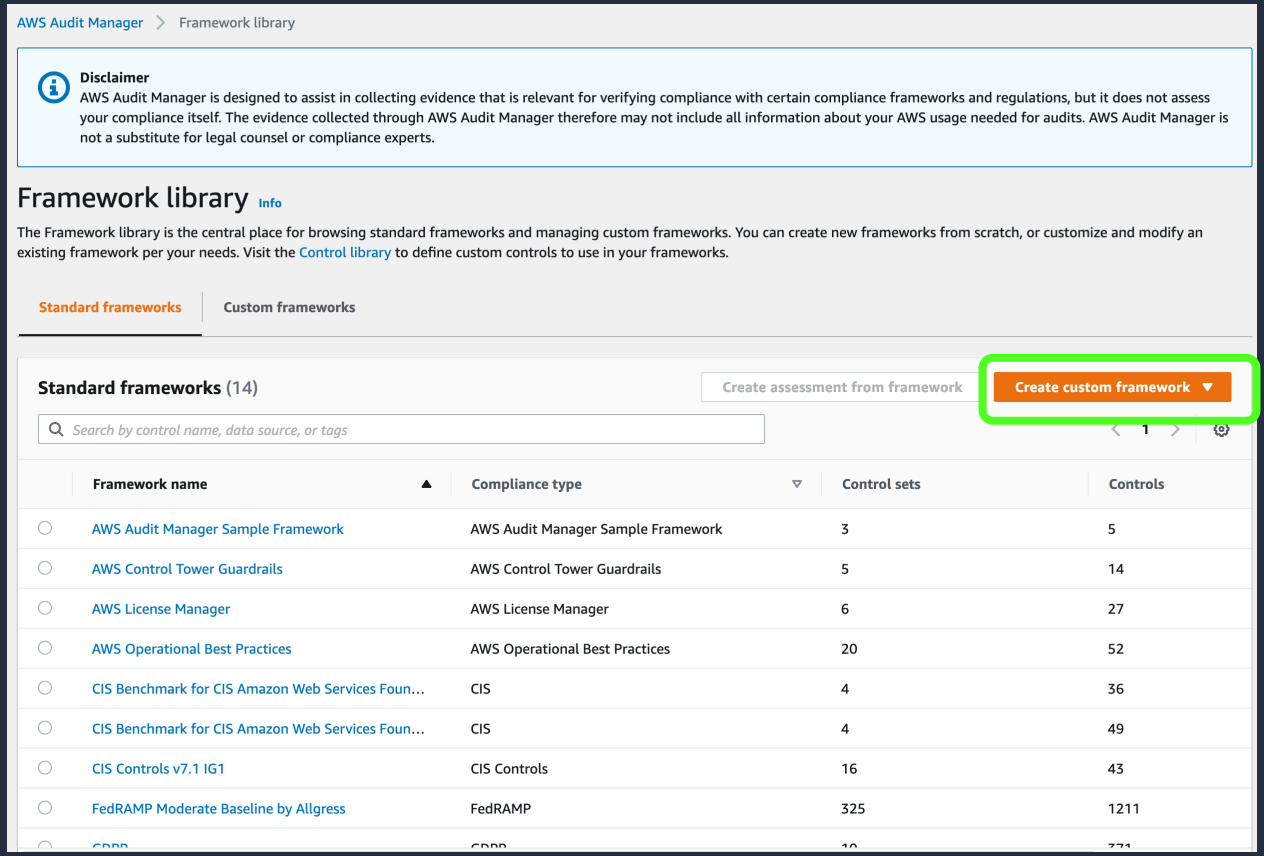
# カスタムコントロールの作成 9



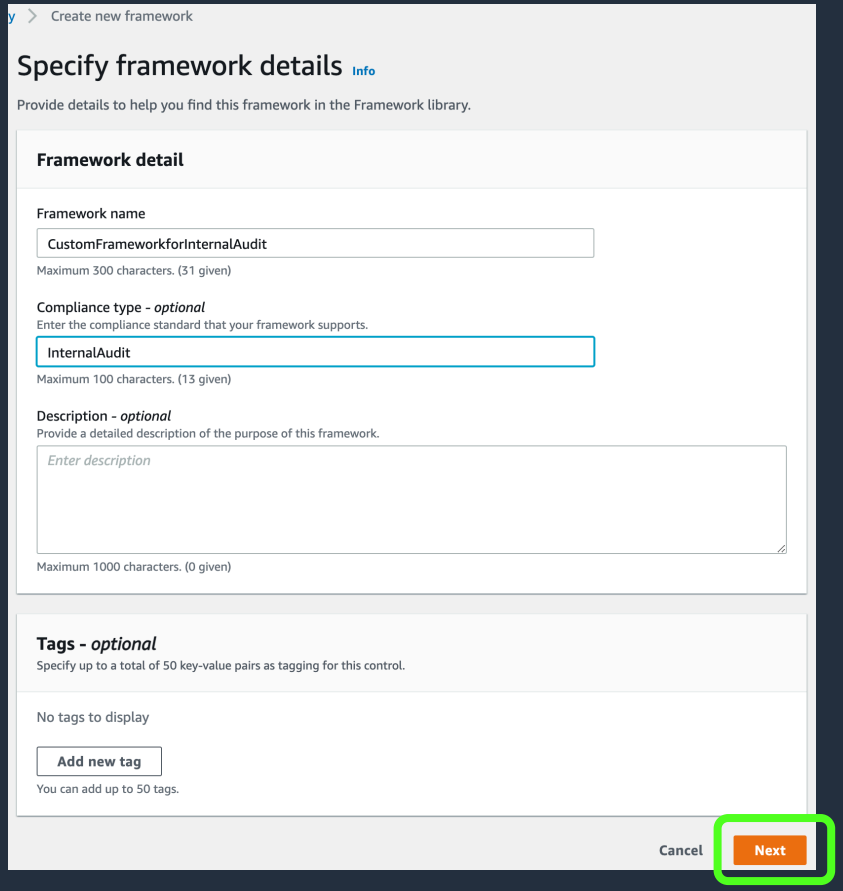
# カスタムフレームワークの作成手順



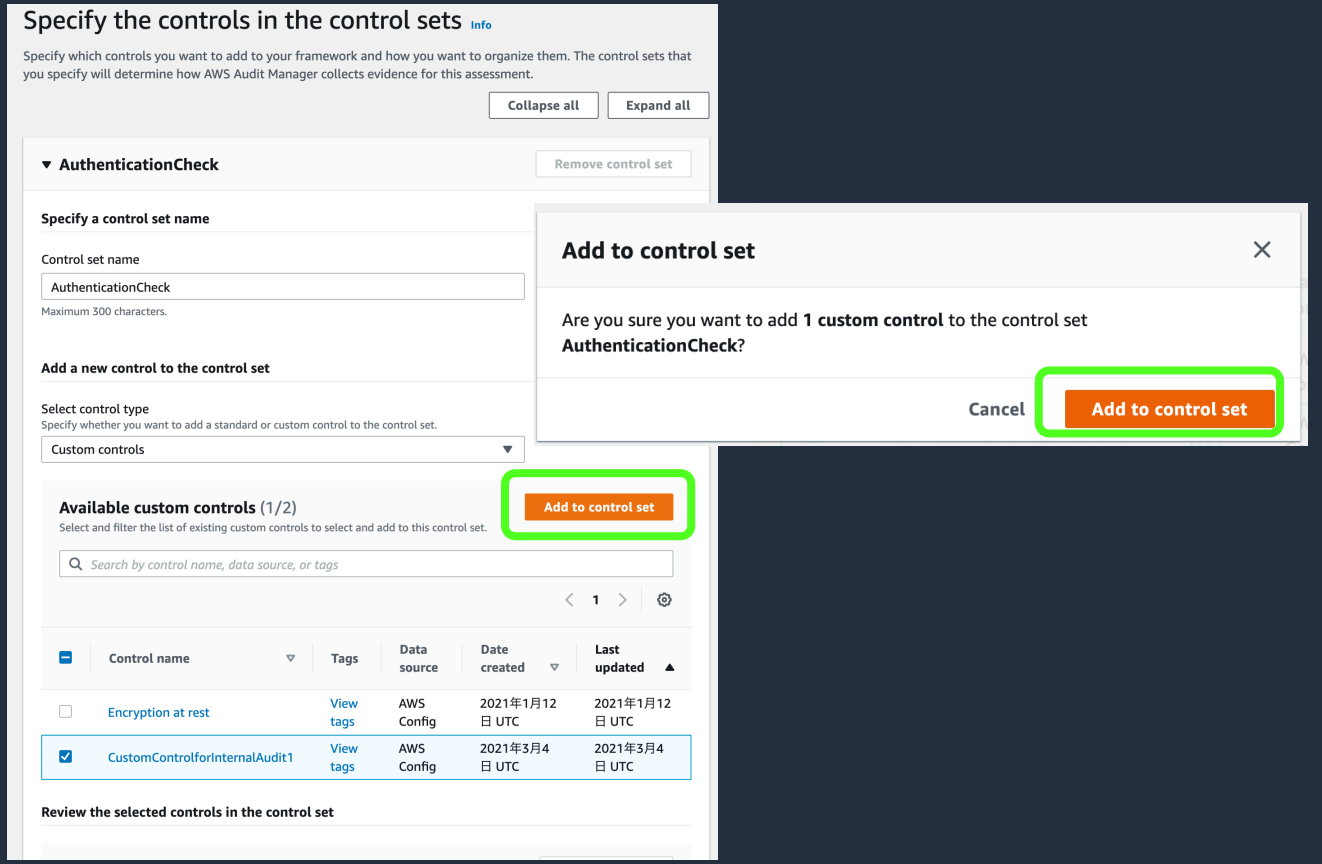
# カスタムフレームワークの作成 1



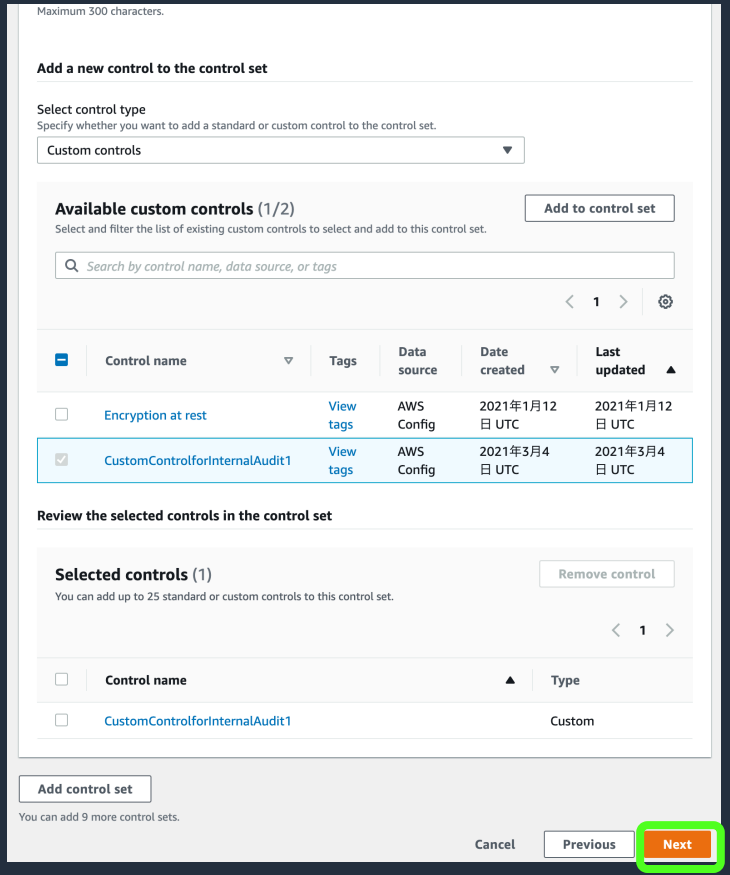
# カスタムフレームワークの作成 2



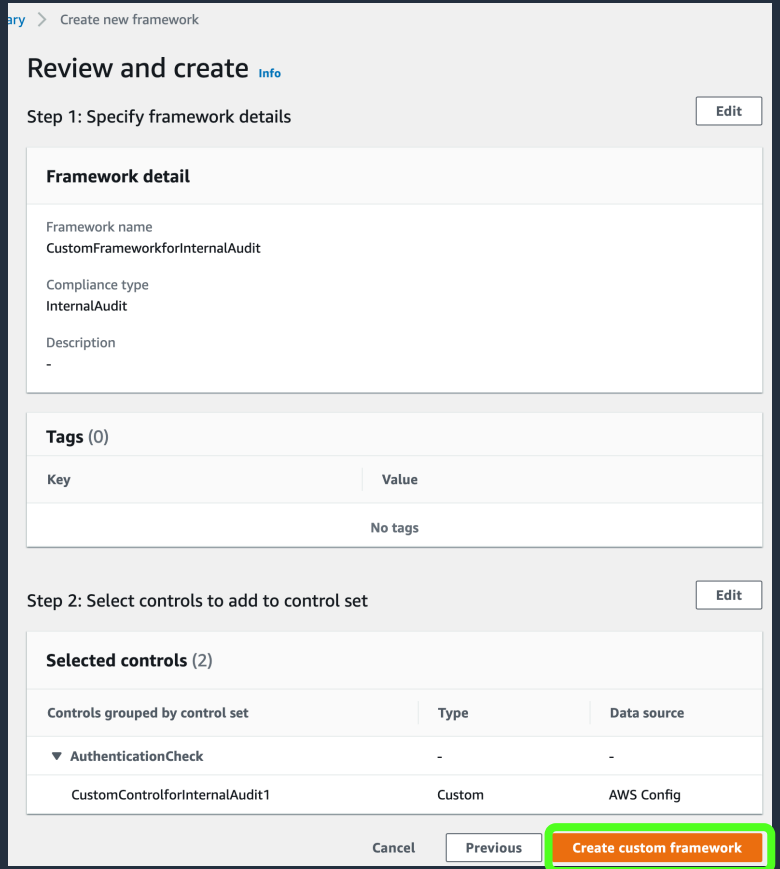
# カスタムフレームワークの作成 3



# カスタムフレームワークの作成 4



# カスタムフレームワークの作成 5

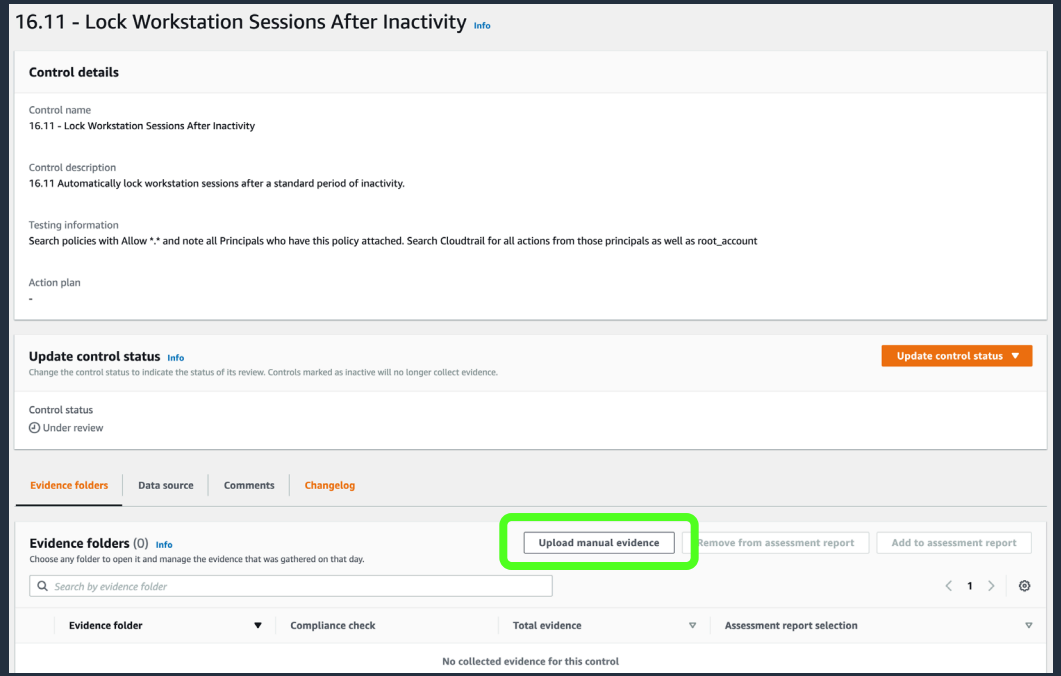


# 手動の証跡/エビデンスのアップロード

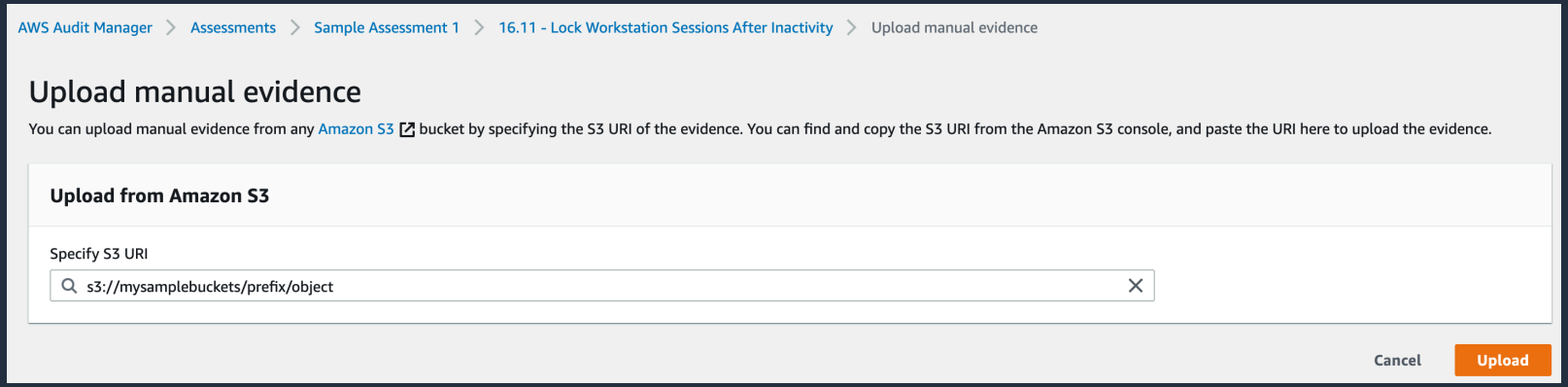
AWS Audit Manager がサポートしていない AWS リソースや、運用体制など AWS 上の設定などで証跡が取得出来ない項目について、手動で証跡となるファイルをアップロードしておくことが可能

# 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



# アップロード元のオブジェクトの指定



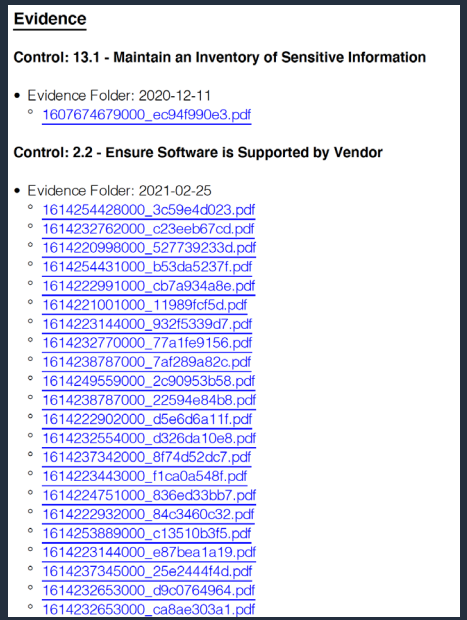
# 評価レポート

- 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



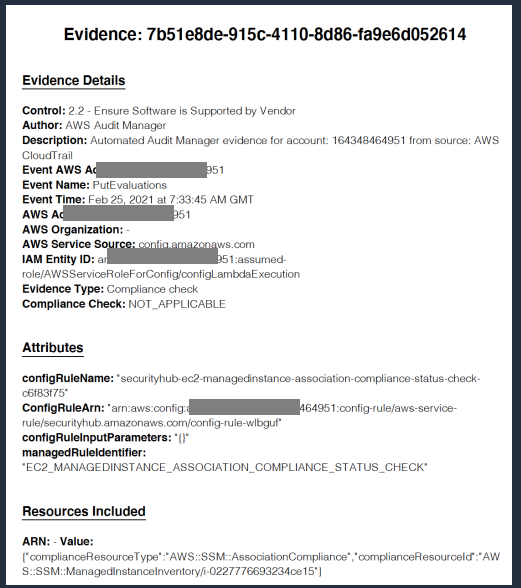
**Evidence**

**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_11989fcf5d.pdf
  - 1614223144000_932f5339d7.pdf
  - 1614232770000_77a1fe9156.pdf
  - 1614238787000_7af289a82c.pdf
  - 1614249559000_2c90953b58.pdf
  - 1614238787000_22594e84b8.pdf
  - 1614222902000_d5e6d6a11f.pdf
  - 1614232554000_d326da10e8.pdf
  - 1614237342000_8f74d52dc7.pdf
  - 1614223443000_f1ca0a548f.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 Ac**[redacted]951
**Event Name:** PutEvaluations
**Event Time:** Feb 25, 2021 at 7:33:45 AM GMT
**AWS Ac**[redacted]951
**AWS Organization:** -
**AWS Service Source:** config.amazonaws.com
**IAM Entity ID:** a[redacted]951:assumed-role/AWSServiceRoleForConfig/configLambdaExecution
**Evidence Type:** Compliance check
**Compliance Check:** NOT_APPLICABLE

**Attributes**

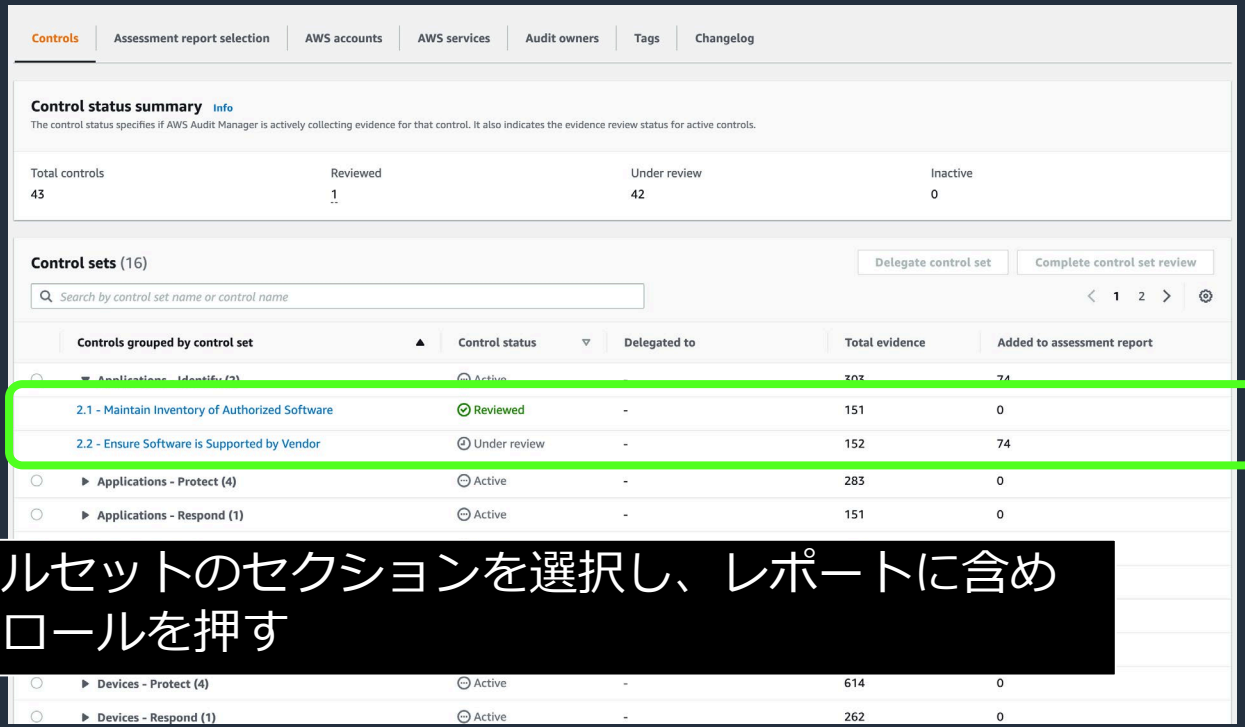
**configRuleName:** "securityhub-ec2-managedinstance-association-compliance-status-check-c6f83f75"
**ConfigRuleArn:** "arn:aws:config:[redacted]464951:config-rule/aws-service-rule/securityhub.amazonaws.com/config-rule-wlbguf"
**configRuleInputParameters:** "{}"
**managedRuleIdentifier:**
"EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK"

**Resources Included**

**ARN:** - **Value:**
{"complianceResourceType":"AWS::SSM::AssociationCompliance","complianceResourceId":"AWS::SSM::ManagedInstanceInventory/i-0227776693234ce15"}

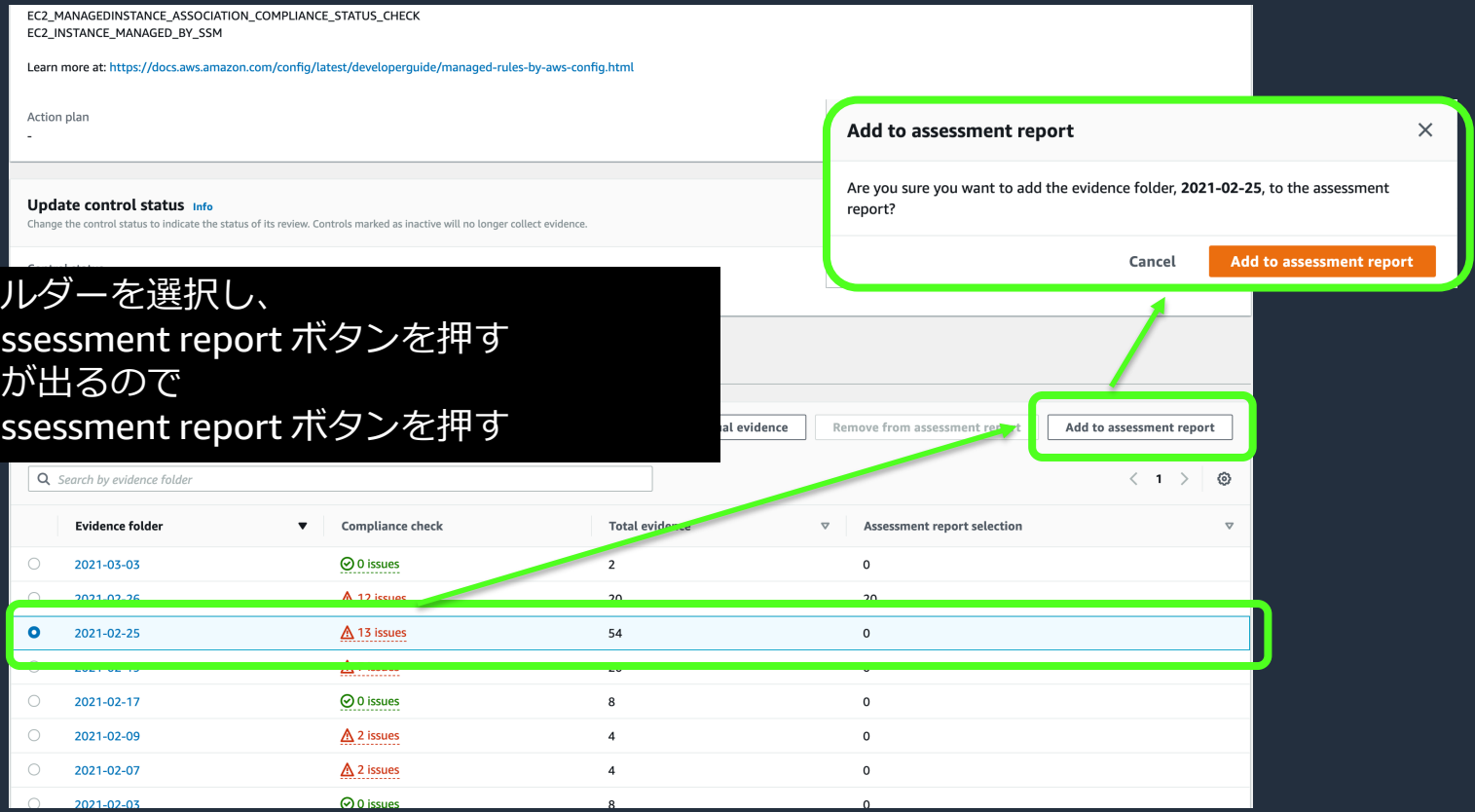
# 評価レポートの作成 1

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




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

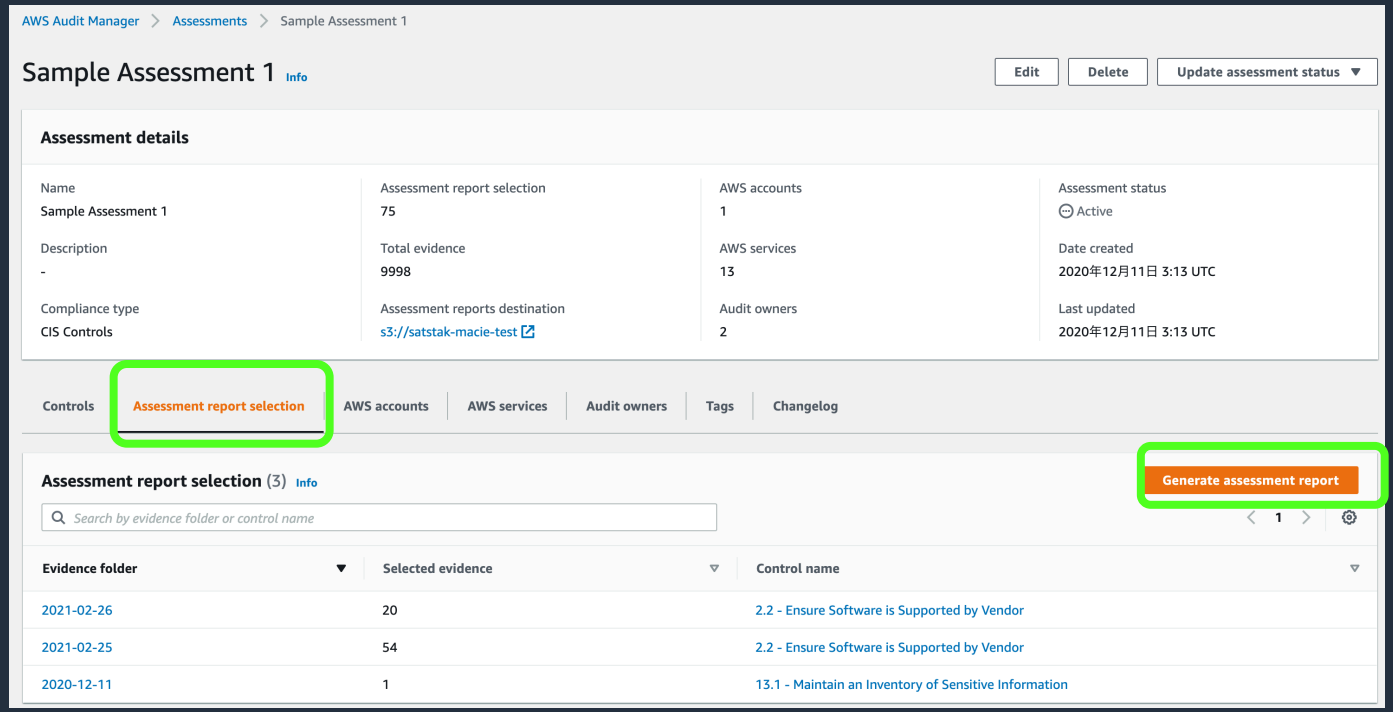
# 評価レポートの作成 2



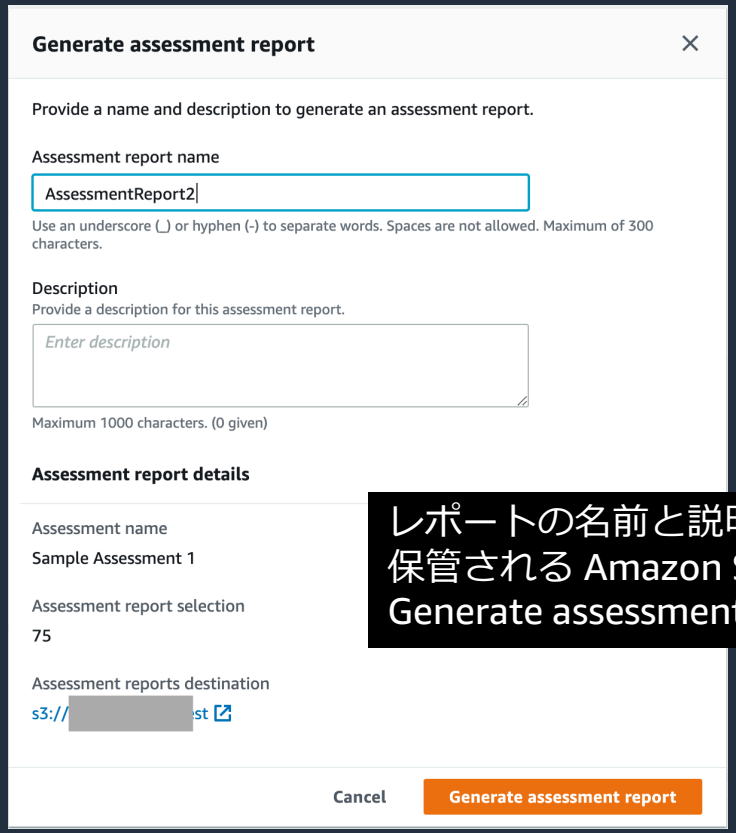

証跡フォルダーを選択し、
Add To assessment report ボタンを押す
確認画面が出るので
Add To assessment report ボタンを押す

# 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



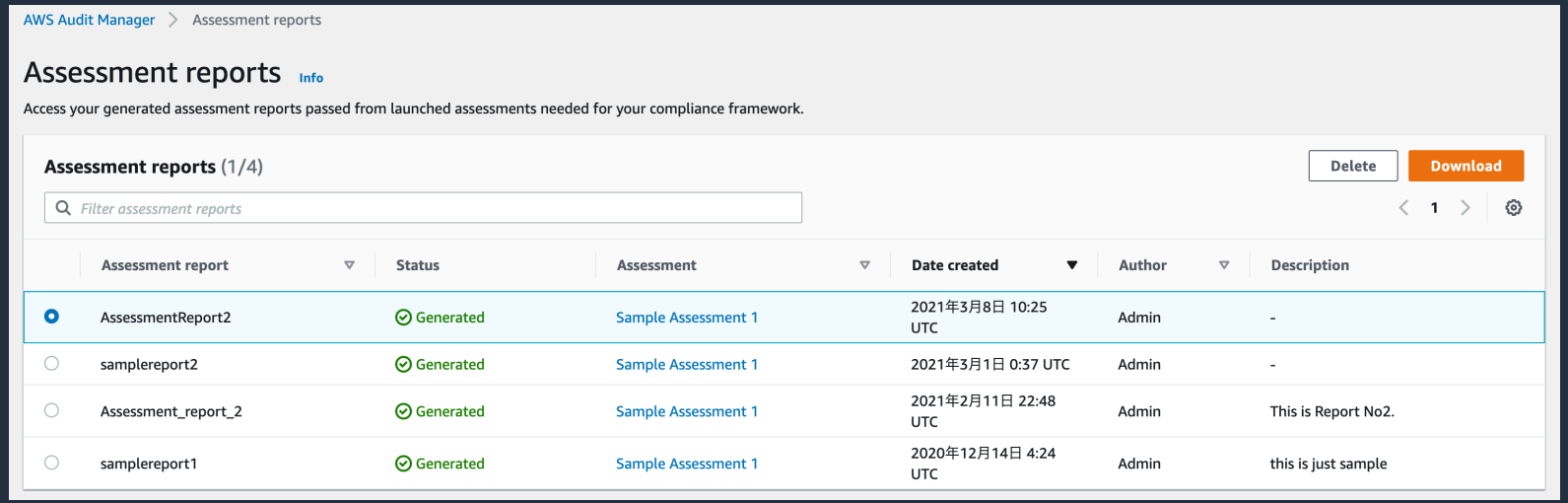
# 評価レポートの作成 4




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

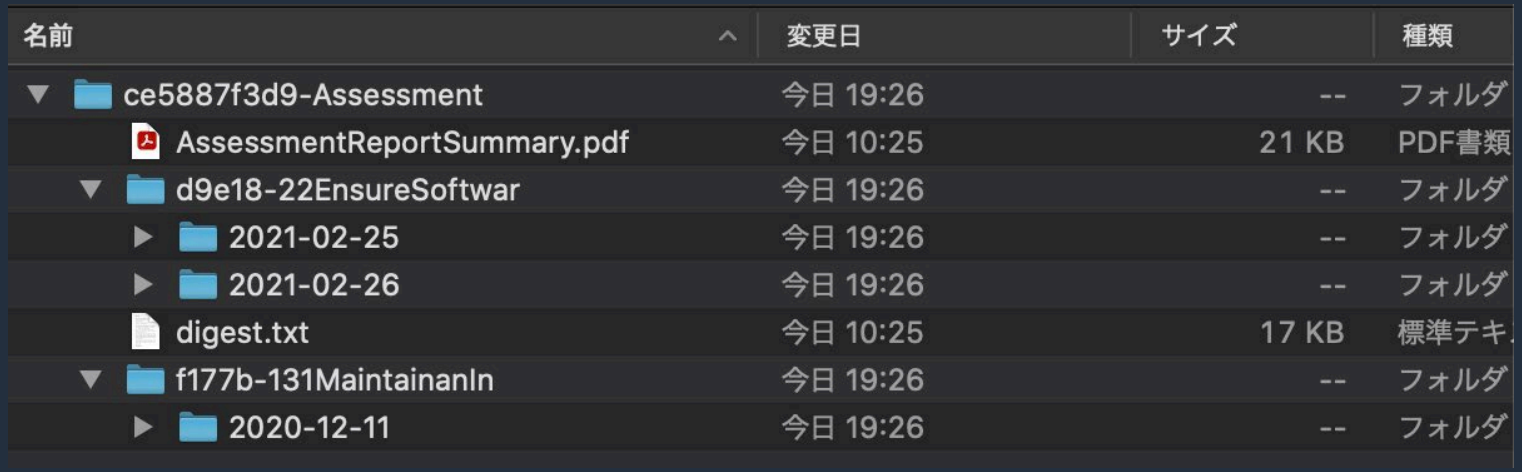
# 評価レポートの作成 5

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



# 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）

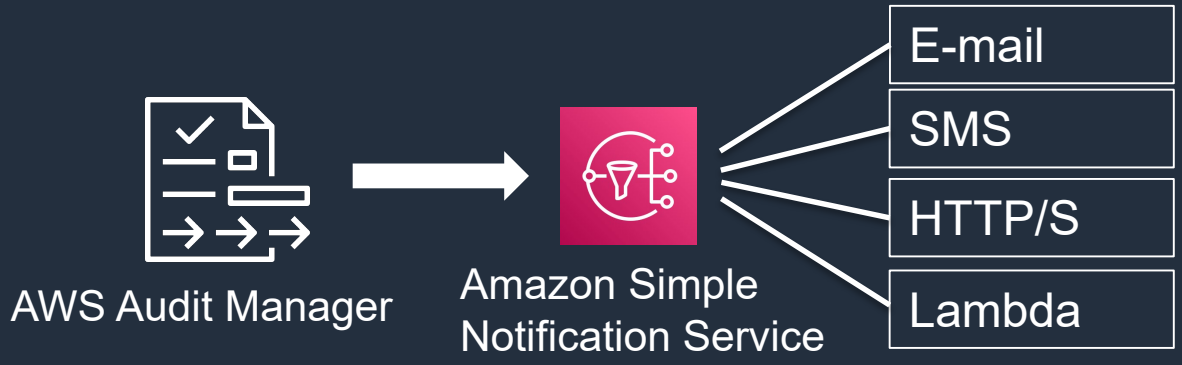


# Audit Manager からの通知

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<br>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、ユーザーのアクテビティ（CloudTrail）、インスタンスなどが 1 つづつカウントされる

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 が一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

- クオータ
    - 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












aws

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


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