aws

ユーザーガイド

# AWS Well-Architected Tool

# AWS Well-Architected Tool: ユーザーガイド

# Table of Contents

# AWS Well-Architected Tool とは

AWS Well-Architected Tool (AWS WA Tool) は、AWS のベストプラクティスを使用してアーキテクチャを測定するための一貫したプロセスを提供するクラウド内のサービスです。AWS WA Tool は、以下を実行することで製品ライフサイクル全体を支援します。

- 決定事項のドキュメント化を支援する
- ベストプラクティスに基づいてワークロードを改善するための推奨事項を提供する
- ワークロードの信頼性、安全性、効率性、費用対効果の向上

AWS WA Tool を使用すると、AWS Well-Architected フレームワークのベストプラクティスを使用して、ワークロードを文書化して測定します。これらのベストプラクティスは、AWS ソリューションアーキテクトがさまざまなビジネスでソリューションを構築してきた長年の経験を基に開発されています。このフレームワークは、アーキテクチャを測定するための一貫したアプローチを提供します。また、時間の経過とともにニーズに応じてスケーリングする設計を実装するのに役立つガイダンスも提供します。

AWS のベストプラクティスに加えてカスタムレンズを使用することで、独自のベストプラクティスに照らしてワークロードを測定できます。カスタムレンズ内の質問は、特定のテクノロジーに特化したり、組織内のガバナンスニーズに対応したりできるようにカスタマイズできます。カスタムレンズは、AWS レンズが提供するガイダンスを補足するものです。

AWS Trusted Advisor と AWS Service Catalog AppRegistry を統合することで、AWS Well-Architected Tool のレビューに関する質問に回答するために必要な情報をより簡単に見つけることができます。

このサービスは、最高技術責任者 (CTO)、アーキテクト、デベロッパー、運用チームのメンバーなど、技術的な製品開発に携わる方を対象としています。AWS のお客様は、アーキテクチャの文書化、製品起動のガバナンス、テクノロジーポートフォリオのリスクの把握と管理のために AWS WA Tool を利用しています。

トピック

- AWS Well-Architected フレームワークとは
- AWS Well-Architected Tool 用語集

# AWS Well-Architected フレームワークとは

AWS Well-Architected フレームワークは、特定のアーキテクチャがクラウドのベストプラクティスにどの程度沿っているかを判断するための、一連の基本的な質問をドキュメント化しています。このフレームワークは、最新のクラウドベースのシステムに要求される品質に対してシステムを評価する一貫したアプローチを提供します。アーキテクチャの状態に基づいて、フレームワークはこれらの品質をより良く達成するために改善できることを提案します。

このフレームワークを使用することで、信頼性、セキュリティ、効率、コスト効果が高いシステムを設計し、クラウド内で運用するためのアーキテクチャのベストプラクティスを学習できます。また、このフレームワークは、ベストプラクティスに照らしてアーキテクチャを評価し、改善すべき分野を特定する一貫した方法を提供します。このフレームワークは、運用上の優秀性、セキュリティ、信頼性、パフォーマンス効率、コスト最適化および持続可能性という 6 本の柱を基本としています。

ワークロードの設計時には、ビジネスニーズに基づいてこれらの柱間でトレードオフを行います。これらのビジネス上の意思決定は、エンジニアリングの優先順位決定を促進する助けになります。開発環境では、信頼性を犠牲にして、コストを削減 (最適化) する場合があります。ミッションクリティカルなソリューションでは、コストの増加を受け入れて、信頼性を最適化する場合があります。e コマースソリューションでは、顧客満足度が収益の増加を促進する可能性があるため、パフォーマンスを優先する場合があります。セキュリティおよび運用上の優秀性は通常、他の柱に対してトレードオフされることはありません。

フレームワークの詳細については、AWSWell-Architected ウェブサイトを参照してください。

# AWS Well-Architected Tool 用語集

以下は、AWS WA Tool および AWS Well-Architected フレームワークでよく使用される用語の定義です。

- ワークロードでは、ビジネス価値をもたらす一連のコンポーネントが特定されます。ワークロードは通常、ビジネスとテクノロジーのリーダーが詳細に話し合う対象です。ワークロードの例には、マーケティングウェブサイト、e コマースウェブサイト、モバイルアプリのバックエンド、分析プラットフォームが含まれます。ワークロードは、アーキテクチャの複雑さのレベルによって異なります。静的ウェブサイトのようにシンプルなものになる場合も、複数のデータストアと多数のコンポーネントで構成されるマイクロサービスアーキテクチャのように複雑なものになる場合もあります。
- マイルストーンは、製品のライフサイクル (設計、テスト、稼働開始、本番稼働) を通じて進化するアーキテクチャの重要な変化を示すものです。

- レンズは、ベストプラクティスに照らしてアーキテクチャを評価し、改善すべき分野を特定する一貫した方法を提供します。

  AWS が提供するレンズに加えて、独自のレンズを作成して使用したり、共有されたレンズを使用したりすることもできます。
- 高リスクの問題 (HRI) は、ビジネスに重大な悪影響を及ぼす可能性があると AWS が認識した、アーキテクチャおよび運用上の選択肢です。HRI は、組織の運用、資産、個人に影響を及ぼす可能性があります。
- 中リスクの問題 (MRI) は、ビジネスに悪影響を及ぼす可能性があると AWS が認識した、アーキテクチャおよび運用上の選択肢ですが、その程度は HRI より低くなります。

  詳細については、「高リスクの問題 (HRI) と中リスクの問題 (MRI)」を参照してください。

# AWS Well-Architected Tool の開始方法

AWS Well-Architected Tool の使用を開始するには、まずユーザー、グループ、ロールに適切なアクセス許可を付与し、AWS WA Tool で使用する AWS のサービスのサポートを有効にします。次に、ワークロードを定義してドキュメント化します。ワークロードの現在の状態のマイルストーンを保存することもできます。

次のトピックでは、AWS WA Tool の使用を開始する方法について説明します。AWS Well-Architected Tool の使用方法を示すステップバイステップのチュートリアルについては、「チュートリアル: AWS Well-Architected Tool ワークロードをドキュメント化する」を参照してください。

トピック



# ユーザー、グループ、ロールに AWS WA Tool へのアクセスを提供する

ユーザー、グループ、またはロールに、AWS Well-Architected Tool へのフルコントロールアクセスまたは読み取り専用アクセスを付与できます。

AWS WA Tool へのアクセスの提供

1. アクセス権限を付与するにはユーザー、グループ、またはロールにアクセス許可を追加します。

   - AWS IAM アイデンティティセンター のユーザーとグループ:

     アクセス許可セットを作成します。「AWS IAM アイデンティティセンター ユーザーガイド」の「アクセス許可セットを作成する」の手順に従ってください。
   - IAM 内で、ID プロバイダーによって管理されているユーザー:

ID フェデレーションのロールを作成します。詳細については IAM ユーザーガイド の サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する を参照してください。

- IAM ユーザー:
  - ユーザーが担当できるロールを作成します。手順については IAM ユーザーガイド の IAM ユーザーのロールの作成 を参照してください。
  - (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加します。「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス許可の追加」の手順を実行します。

2. フルコントロールを許可するには、WellArchitectedConsoleFullAccess マネージドポリシーをアクセス許可一式またはロールに適用します。

   フルアクセスを許可することで、プリンシパルが AWS WA Tool ですべてのアクションを実行できるようになります。このアクセスは、ワークロードの定義、ワークロードの削除、ワークロードの表示、ワークロードの更新、ワークロードの共有、カスタムレンズの作成、カスタムレンズの共有に必要です。

3. 読み取り専用アクセスを許可するには、WellArchitectedConsoleReadOnlyAccess マネージドポリシーをアクセス許可セットまたはロールに適用します。このロールを持つプリンシパルは、リソースを表示することしかできません。

これらのポリシーの詳細については、「AWS の マネージドポリシーAWS Well-Architected Tool」を参照してください。

# AWS WA Tool での他の AWS サービスのサポートの有効化

組織アクセスを有効にすると、AWS Well-Architected Tool は組織の構造に関する情報を収集して、リソースをより簡単に共有できるようになります (詳細については、「the section called “AWS Organizations 内でリソース共有を有効にする”」を参照してください)。Discovery サポートの有効化により、AWS Trusted Advisor、AWS Service Catalog AppRegistry、関連リソース (AppRegistry リソースコレクションの CloudFormation スタックなど) から情報を収集することで、Well-Architected レビュー関連の質問の回答に必要な情報を簡単に検出でき、ワークロードの Trusted Advisor のチェックをカスタマイズできます。

AWS Organizations のサポートを有効化するか、Discovery サポートを有効化にすると、アカウントに対するサービスにリンクされたロールを自動作成できます。

AWS WA Tool が相互作用できる他のサービスのサポートをオンにするには、[設定] に移動します。

1. AWS Organizations から情報を収集するには「AWS Organizations のサポートを有効化」をオンにします。
2. [Discovery サポートの有効化] をオンにすると、その他 AWS サービスとリソースから情報を収集できます。
3. [ロールの許可を表示] を選択して、サービスにリンクされたロールアクセス許可または信頼関係ポリシーを確認します。
4. [設定を保存] を選択します。

## ワークロードの AppRegistry のアクティブ化

AppRegistry の使用はオプションであり、AWS ビジネスサポートおよびエンタープライズサポートのお客様はワークロードごとにアクティブ化できます。

Discovery のサポートが有効になっていて、AppRegistry が新規または既存のワークロードに関連付けられると、AWS Well-Architected Tool はサービス管理属性グループを作成します。AppRegistry の属性グループであるメタデータには、ワークロード ARN、ワークロード名、ワークロードに関連付けられたリスクが含まれます。

- Discovery サポートをオンにすると、ワークロードが変更されるたびに、属性グループが更新されます。
- Discovery サポートがオフになるか、アプリケーションがワークロードから削除されると、ワークロード情報は AWS Service Catalog から削除されます。

Trusted Advisor からフェッチしたデータを AppRegistry アプリケーションで起動したい場合、ワークロードの [リソース定義] を [AppRegistry] または [すべて] に設定します。the section called “IAM で Trusted Advisor を有効化” のガイドラインに従って、アプリケーションでリソースを保有するすべてのアカウントに対するロールを作成します。

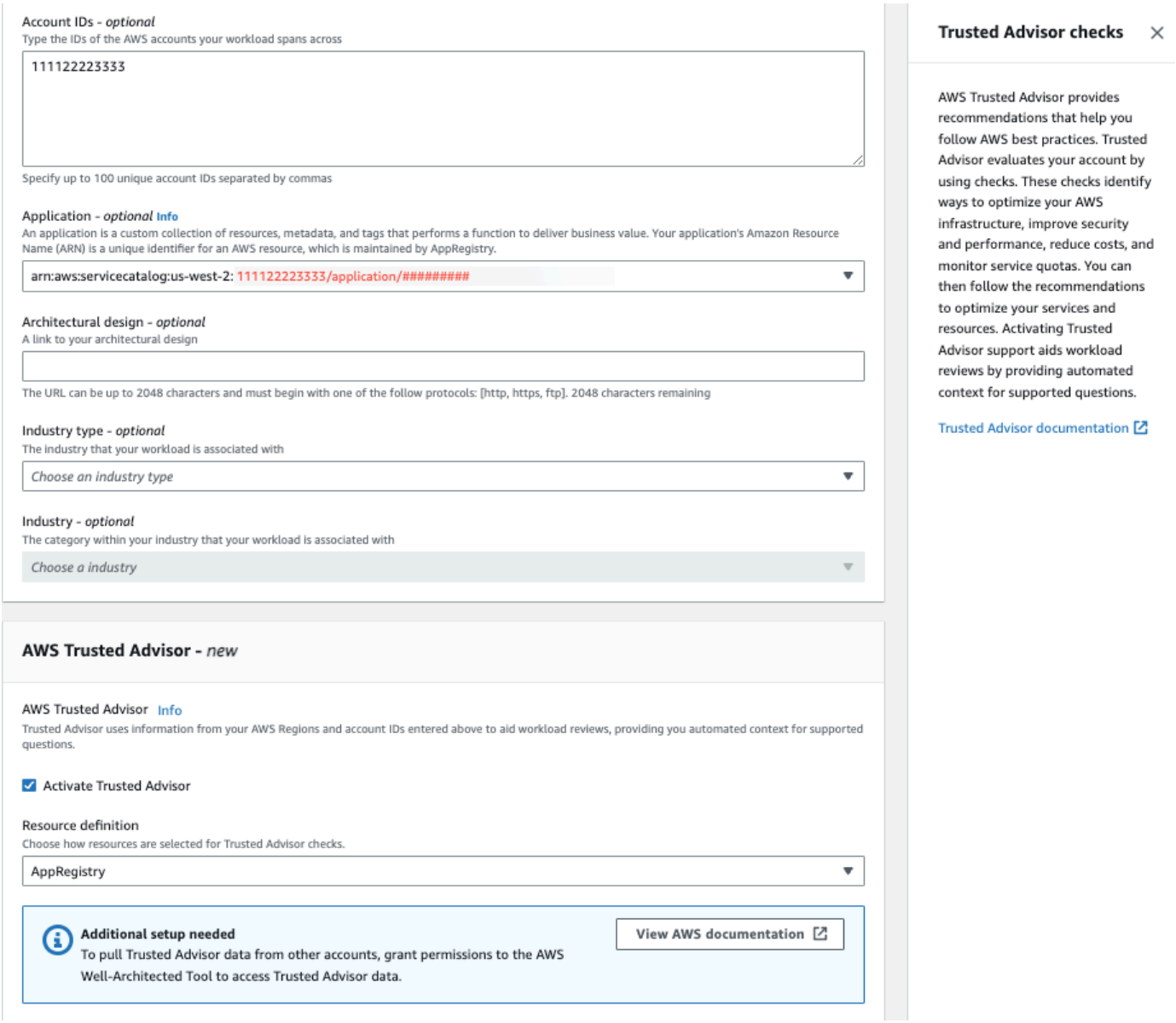
## ワークロードの AWS Trusted Advisor のアクティブ化

AWS ビジネスサポートおよびエンタープライズサポートのお客様は、必要に応じて AWS Trusted Advisor と統合し、ワークロードごとにアクティブ化できます。Trusted Advisor とAWS WA Tool の統合には費用はかかりませんが、Trusted Advisor の価格詳細については、「AWS サポートプラン」を参照してください。ワークロードに対して Trusted Advisor をアクティブ化すると、AWS ワークロードのレビューと最適化に、自動化とモニタリングに対応するより包括的なアプローチを提供でき

ます。これにより、ワークロードの信頼性、セキュリティ、パフォーマンス、コスト最適化を向上させることができます。

ワークロードの Trusted Advisor をアクティブ化する

1. Trusted Advisor をアクティブ化するには、ワークロード所有者は、AWS WA Tool を使用して、既存のワークロードを更新するか、[ワークロードの定義] を選択して新しいワークロードを作成します。
2. Trusted Advisor を有効にするには、[アカウント ID] フィールドに Trusted Advisor で使用するアカウント ID を入力するか、[アプリケーション] フィールドでアプリケーション ARN を選択するか、またはその両方を実行します。
3. [AWS Trusted Advisor] セクションで [Trusted Advisor をアクティブ化する] を選択します。



4. Trusted Advisor がワークロードに対して初めてアクティブ化されると、 IAM サービスロールが作成される旨の通知が表示されます。[許可を表示] を選択すると、IAM ロールのアクセス許可が表示されます。JSON が IAM で自動作成したロール名、アクセス許可および信頼関係を閲覧できます。ロールが作成されたら、Trusted Advisor をアクティブ化する後続のワークロードでは、[追加のセットアップが必要です] という通知が表示されます。
5. [リソース定義] ドロップダウンでは、[ワークロードメタデータ]、[AppRegistry]、または [すべて] を選択できます。リソース定義の選択では、Well-Architected のベストプラクティスに対応するワークロードレビューのステータスチェックを行うために、AWS WA Tool がどのデータを Trusted Advisor から取得するかを定義します。

   ワークロードメタデータ — ワークロードはアカウント ID によって定義され、AWS リージョンは、ワークロード内で指定されます。

   AppRegistry — ワークロードは、ワークロードに関連付けられた AppRegistry アプリケーションに存在するリソース (CloudFormation スタックなど) によって定義されます。

   すべて — ワークロードはワークロードメタデータと AppRegistry リソースの両方によって定義されます。
6. [次へ] を選択します。
7. AWS Well-Architected フレームワークをワークロードに適用して、[ワークロードの定義] を選択します。Trusted Advisor のチェックは、AWS Well-Architected フレームワークのみにリンクしており、その他レンズにはリンクしていません。

AWS WA Tool は IAM で作成されたロールを使用して、Trusted Advisor から定期的にデータを取得します。IAM ロールはワークロード所有者用に自動作成されます。ただし、Trusted Advisor 情報を表示するには、ワークロード上の関連アカウントの所有者が IAM にアクセスしてロールを作成する必要があります。詳細については、「???」を参照してください。このロールが存在しない場合、AWS WA Tool は、そのアカウントの Trusted Advisor 情報を取得できず、エラーが表示されます。

AWS Identity and Access Management (IAM) でのロール作成の詳細については、「IAM ユーザーガイド」の「AWS サービス用ロールの作成 (コンソール)」を参照してください。

## ワークロードに対して IAM で Trusted Advisor を有効化

> **Note**
>
> ワークロードの所有者は、Trusted Advisor ワークロードを作成する前に、自分のアカウントの Discovery サポートの有効化を実行する必要があります。[Discovery サポートの有効化] を選択すると、ワークロード所有者に必要なロールが作成されます。他のすべての関連アカウントには、以下の手順を使用してください。

Trusted Advisor が有効化されたワークロードの関連アカウントの所有者は、AWS Well-Architected Tool で Trusted Advisor 情報を確認するために、IAM でロールを作成する必要があります。

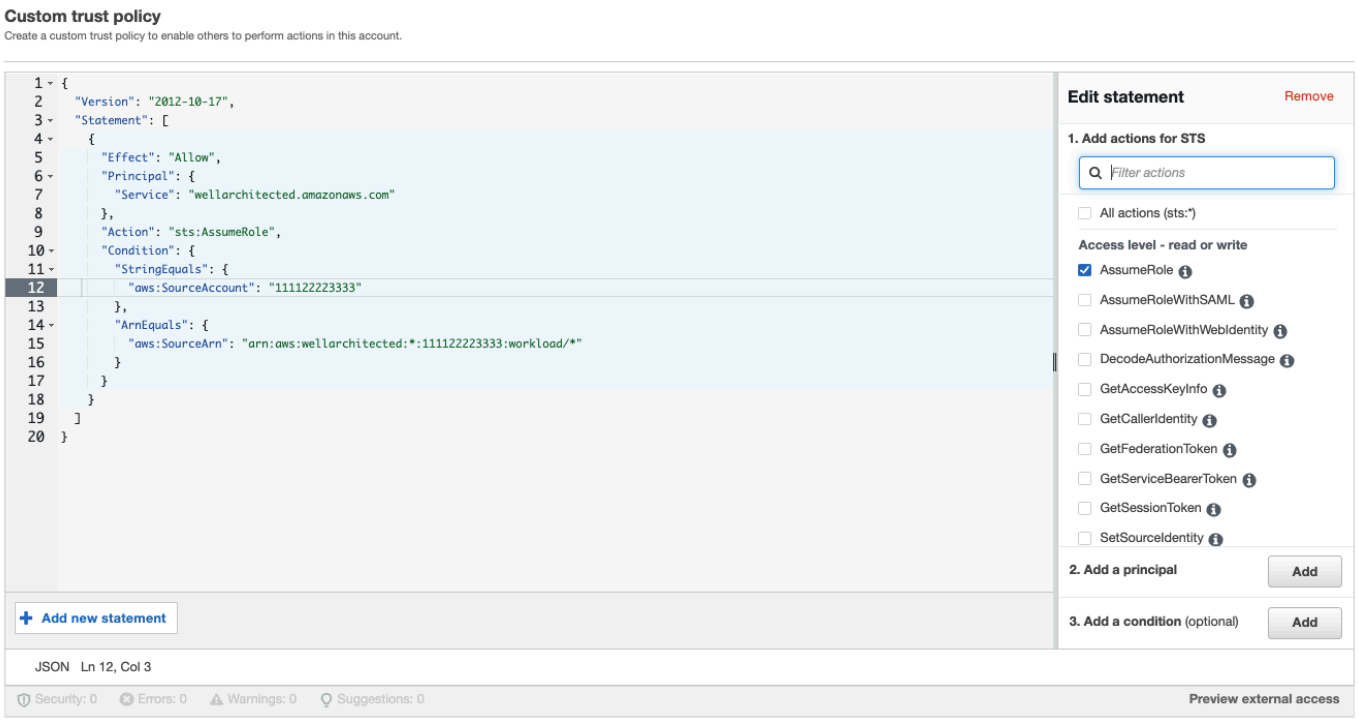
AWS WA Tool が Trusted Advisor から情報を取得するために IAM でロールを作成する

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
2. IAM コンソールのナビゲーションペインで、[ロール]、[ロールを作成] の順に選択します。
3. [信頼されたエンティティのタイプ] で、[カスタム信頼ポリシー] を選択します。
4. 次の図に示すように、次のカスタム信頼ポリシーをコピーして IAM コンソールの JSON フィールドに貼り付けます。*WORKLOAD_OWNER_ACCOUNT_ID* をワークロード所有者のアカウント ID に置き換え、[次へ] を選択します。

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "wellarchitected.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "WORKLOAD_OWNER_ACCOUNT_ID"
                },
                "ArnEquals": {
```

```
                    "aws:SourceArn":
 "arn:aws:wellarchitected:*:111122223333:workload/*"
                }
            }
        }
    ]
}
```




> **Note**
>
> 前述のカスタム信頼ポリシーの条件ブロックの aws:sourceArn は、"arn:aws:wellarchitected:*:*WORKLOAD_OWNER_ACCOUNT_ID*:workload/*" です。これは、ワークロード所有者のすべてのワークロードに対してAWS WA Toolがこのロールを使用できることを示す一般的な条件です。ただし、アクセスを特定のワークロード ARN または一連のワークロード ARN に絞り込むことができます。複数の ARN を指定するには、次の信頼ポリシーの例を参照してください。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "wellarchitected.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                "aws:SourceAccount": "111122223333"
                },
                "ArnEquals": {
                    "aws:SourceArn": [
                    "arn:aws:wellarchitected:us-
east-1:111122223333:workload/WORKLOAD_ID_1",
    "arn:aws:wellarchitected:us-
east-1:111122223333:workload/WORKLOAD_ID_2"
                    ]
                }
            }
        }
    ]
}
```

5. [アクセス許可の追加] ページで [アクセス許可ポリシー] に対して、[ポリシーの作成] を選択し、Trusted Advisor からデータの読み取るアクセスを AWS WA Tool に付与します。[ポリシーの作成] を選択すると、新しいウィンドウが開きます。

> **Note**
>
> さらに、ロール作成中はアクセス許可の作成を省略し、ロールの作成後にインラインポリシーを作成することもできます。ロールが正常に作成された旨を示すメッセージで [ロールを表示] をクリックし、[アクセス許可] タブの [アクセス許可の追加] ドロップダウンから [インラインポリシーの作成] を選択します。

6. 以下のアクセス許可ポリシーをコピーして、[JSON] フィールドに貼り付けます。Resource ARN で、*YOUR_ACCOUNT_ID* を自分のアカウント ID に置き換え、リージョンまたはアスタリスク (*) を指定して、[次へ: タグ] を選択します。

   ARN 形式の詳細については、「 AWS の一般的なリファレンスガイド」の「Amazon リソースネーム (ARN)」を参照してください。

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:DescribeCheckRefreshStatuses",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeRiskResources",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeRisk",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeRisks",
                "trustedadvisor:DescribeCheckItems"
            ],
            "Resource": [
                "arn:aws:trustedadvisor:*:111122223333:checks/*"
            ]
        }
    ]
}
```

7. Trusted Advisor がワークロードに対して有効化され、[リソース定義] が [AppRegistry] または [すべて] に設定されている場合、ワークロードにアタッチされている AppRegistry アプリケーション内のリソースを所有するすべてのアカウントは、Trusted Advisor ロールの [アクセス許可ポリシー] に次のアクセス許可を追加する必要があります。

   JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "DiscoveryPermissions",
            "Effect": "Allow",
            "Action": [
                "servicecatalog:ListAssociatedResources",
                "tag:GetResources",
                "servicecatalog:GetApplication",
                "resource-groups:ListGroupResources",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStackResources"
            ],
            "Resource": "*"
        }
    ]
}
```

8. (オプション) タグを追加します。[次へ: レビュー] を選択します。
9. ポリシーが正しいことを確認したら、名前を付けて、[ポリシーの作成] を選択します。
10. ロールの [アクセス許可の追加] ページで、作成したポリシー名を選択し、[次へ] を選択します。
11. `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* の構文に沿ったロール名を入力し、[ロールを作成] を選択します。*`WORKLOAD_OWNER_ACCOUNT_ID`* をワークロード所有者のアカウント ID に置き換えます。

    ページ上部にロールが正常に作成されたことを知らせるメッセージが表示されます。
12. ロールと関連するアクセス許可ポリシーを表示するには、左側のナビゲーションペインの [アクセス管理] で [ロール] を選択し、`WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* の名前を検索します。ロールの名前を選択して、[アクセス許可] と [信頼関係] が正しいことを確認します。

## ワークロードの Trusted Advisor を非アクティブ化する

ワークロードの Trusted Advisor を非アクティブ化するには

ワークロードを編集して、[Trusted Advisor をアクティブ化する] を選択解除すると、AWS Well-Architected Tool から任意のワークロードの Trusted Advisor を非アクティブ化できます。ワークロードの編集に関する詳細は、「the section called “ワークロードの編集”」を参照してください。

AWS WA Tool から Trusted Advisor を非アクティブ化すると、IAM で作成されたロールが削除されます。IAM からロールを削除するには、別のクリーンアップ手段が必要です。ワークロードの所有者または関連するアカウントの所有者は、Trusted Advisor が AWS WA Tool で非アクティブ化されたときに作成された IAM ロールを削除するか、AWS WA Tool による ワークロードの Trusted Advisor データ収集を停止する必要があります。

IAM で **`WellArchitectedRoleForTrustedAdvisor`** を削除するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
2. IAM コンソールのナビゲーションペインで、[ロール] を選択します。
3. `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* を検索して、ロール名を選択します。
4. [削除] を選択します。ポップアップウィンドウで、ロール名を入力して削除を確認したら、もう一度 [削除] を選択します。

IAM からロールを削除する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの削除 (コンソール)」を参照してください。

# AWS WA Tool でのワークロードの定義

ワークロードとは、ビジネス価値をもたらすコンポーネントのセットです。例えば、ワークロードには、マーケティングウェブサイト、e コマースウェブサイト、モバイルアプリのバックエンド、分析プラットフォームがあります。ワークロードを正確に定義すると、AWS Well-Architected フレームワークの柱に対する包括的なレビューを行うことができます。

ワークロードを定義するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. AWS WA Tool を初めて使用すると、サービスの特徴を紹介するページが表示されます。[ワークロードを定義する] セクションで [ワークロードの定義] を選択します。

   あるいは、左側のナビゲーションペインで、[Workloads (ワークロード)]、[Define workload (ワークロードの定義)] の順に選択します。

   AWS がワークロードデータをどのように使用するかの詳細については、[AWS がこのデータを必要とする理由とその用途] を選択します。

3. [Name (名前)] ボックスに、ワークロードの名前を入力します。

> **Note**
>
> 名前は 3 ~ 100 文字にします。3 文字以上をスペースにしないでください。ワークロード名は一意にしてください。一意かどうかを確認するときは、スペースと大文字は無視されます。

4. [Description (説明)] ボックスに、ワークロードの説明を入力します。説明は 3 ~ 250 文字にしてください。
5. [Review owner (レビューの 所有者)] ボックスに、ワークロードのレビュープロセスを所有するプライマリグループまたは個人の名前、E メールアドレス、または識別子を入力します。
6. [環境] ボックスで、ワークロードの環境を選択します。
   - [Production] (本番稼動) – ワークロードは本番稼動環境で実行されます。
   - [Pre-production] (本番稼働前) – ワークロードは本番稼働前環境で実行されます。
7. [リージョン] セクションで、ワークロードのリージョンを選択します。
   - [AWS リージョン]– ワークロードが実行される AWS リージョンを 1 つずつ選択します。
   - AWS 以外の領域 – ワークロードが実行される AWS 以外のリージョン名を入力します。5 つまでの一意のリージョンをカンマで区切って指定できます。

   ワークロードに該当する場合は、両方のオプションを使用します。
8. (オプション) [Account IDs] (アカウント ID) ボックスに、ワークロードに関連付けられている AWS アカウントの ID を入力します。最大 100 個の一意のアカウント ID をカンマで区切って指定できます。

   Trusted Advisor がアクティブ化されると、指定されたアカウント ID が Trusted Advisor からのデータ取得に使用されます。IAM で ユーザーの代わりに Trusted Advisor データを取得するアクセス許可を AWS WA Tool に付与するには、「ワークロードの AWS Trusted Advisor をアクティブ化する」を参照してください。
9. (オプション) [アプリケーション] ボックスに、AWS Service Catalog AppRegistry からこのワークロードに関連付けるアプリケーションのアプリケーション ARN を入力します。各ワークロードに指定できる ARN はひとつだけで、アプリケーションとワークロードは、同じリージョンである必要があります。
10. (オプション) [ Architectural design (アーキテクチャ設計)] ボックスに、アーキテクチャ設計の URL を入力します。

11. (オプション) [Industry type (業界)] ボックスで、ワークロードに関連する業界を選択します。
12. (オプション) [Industry (業種)] ボックスで、ワークロードに最も一致する業種を選択します。
13. (オプション) [Trusted Advisor] セクションで、ワークロードに対して [Trusted Advisor のチェック] をオンにし、[Trusted Advisor をアクティブ化する] を選択します。ワークロードに関連するアカウントには、追加の設定が必要な場合があります。ユーザーの代わりに Trusted Advisor データを取得するアクセス許可を AWS WA Tool に付与するには、「the section called “Trusted Advisor のアクティブ化”」を参照してください。[リソース定義] の [ワークロードメタデータ]、[AppRegistry]、または [すべて] を選択して、AWS WA Tool がTrusted Advisor のチェックを実行するために使用するリソースを定義します。
14. (オプション) ワークロードレベルでワークロードの Jira 同期設定を有効にするには、[Jira] セクションで、[アカウントレベルの設定を上書] を選択します。ワークロードに関連するアカウントには、追加の設定が必要な場合があります。コネクタのセットアップと設定を開始するには、「AWS Well-Architected Tool Connector for Jira」を参照してください。[ワークロードを同期しない]、[ワークロードの同期 - 手動]、[ワークロードの同期 - 自動] から選択し、必要に応じて同期先の [Jira プロジェクトキー] を入力します。

    > **Note**
    >
    > アカウントレベルの設定を上書きしない場合、ワークロードには、デフォルトでアカウントレベルの Jira の同期設定が適用されます。

15. (オプション) [Tags] (タグ) セクションで、ワークロードに関連付けるタグを追加します。

    タグの詳細については、「AWS WA Tool リソースのタグ付け」を参照してください。
16. [次へ] を選択します。

    必須ボックスが空白の場合、または指定した値が無効な場合は、続行する前に問題を修正する必要があります。
17. (オプション) [プロファイルの適用] で、既存のプロファイルを選択するか、プロファイル名を検索するか、[プロファイルの作成] を選択してプロファイルを作成し、プロファイルをワークロードに関連付けます。[次へ] を選択します。
18. このワークロードに適用するレンズを選択します。ワークロードには最大 20 個のレンズを追加できます。公式な AWS レンズの説明については、「レンズ」を参照してください。

    レンズは、[カスタムレンズ] (自分で作成したレンズまたは AWS アカウントと共有したレンズ)、[レンズカタログ] (すべてのユーザーが利用できる公式な AWS レンズ)、またはその両方から選択できます。

> **Note**
>
> カスタムレンズを作成していない場合や、カスタムレンズを共有していない場合、[カスタムレンズ] セクションには何も表示されません。

> **免責事項**
>
> 他の AWS ユーザーまたはアカウントが作成したカスタムレンズにアクセスする、またはそれらを適用する (あるいはその両方) ことで、他のユーザーが作成、共有したカスタムレンズが、AWS カスタマーアグリーメントに定義されているサードパーティーコンテンツであることを認めるものとします。

19. [ワークロードの定義] を選択します。

    必須ボックスが空白の場合、または指定した値が無効な場合は、ワークロードを定義する前に問題を修正する必要があります。

# AWS WA Tool でのワークロードのドキュメント化

AWS Well-Architected Tool でワークロードを定義したら、[ワークロードのレビュー] ページを開くことで、ワークロードの状態をドキュメント化できます。これは、ワークロードを評価し、時間の経過に伴う進行状況を追跡するために役立ちます。

ワークロードの状態をドキュメント化するには

1. 最初にワークロードを定義すると、ワークロードの現在の詳細を示すページが表示されます。[Start reviewing (レビューの開始)] を選択して開始します。

   それ以外の場合は、左側のナビゲーションペインで [Workloads (ワークロード)] を選択してから、ワークロードの名前を選択して、ワークロード詳細ページを開きます。[Continue reviewing (確認を続行)] を選択します。

   (オプション) プロファイルがワークロードに関連付けられている場合、左側のナビゲーションペインには、ワークロードレビュープロセスを加速するために使用できる優先度の高いワークロードレビューの質問リストが表示されます。
2. 最初の質問が表示されます。質問ごとに、以下の手順を実行します。

a. 質問を読み、質問がワークロードに当てはまるかどうかを判断します。

   その他のガイダンスについては、[情報] を選択すると、ヘルプパネルに情報が表示されます。

   - 質問がワークロードに当てはまらない場合は、[Question does not apply to this workload (質問はこのワークロードに当てはまらない)] を選択します。
   - それ以外の場合は、リストから現在従っているベストプラクティスを選択します。

     現在どのベストプラクティスにも従っていない場合は、[None of these (該当なし)] を選択します。

   任意の項目に関するその他のガイダンスについては、[情報] を選択すると、ヘルプパネルに情報が表示されます。

b. (オプション) 1 つ以上のベストプラクティスがワークロードに適用されない場合は、[Mark best practice(s) that don't apply to this workload] (このワークロードに適用されないベストプラクティスをマーク) を選択します。選択したベストプラクティスごとに、オプションで理由を選択し、追加の詳細を指定できます。

c. (オプション) 質問に関する情報を記録するには、[コメント] ボックスを使用します。

   たとえば、質問が当てはまらない理由を説明したり、選択したベストプラクティスに関する追加の詳細を提供したりできます。

d. 次の質問に進むには [Next (次へ)] を選択します。

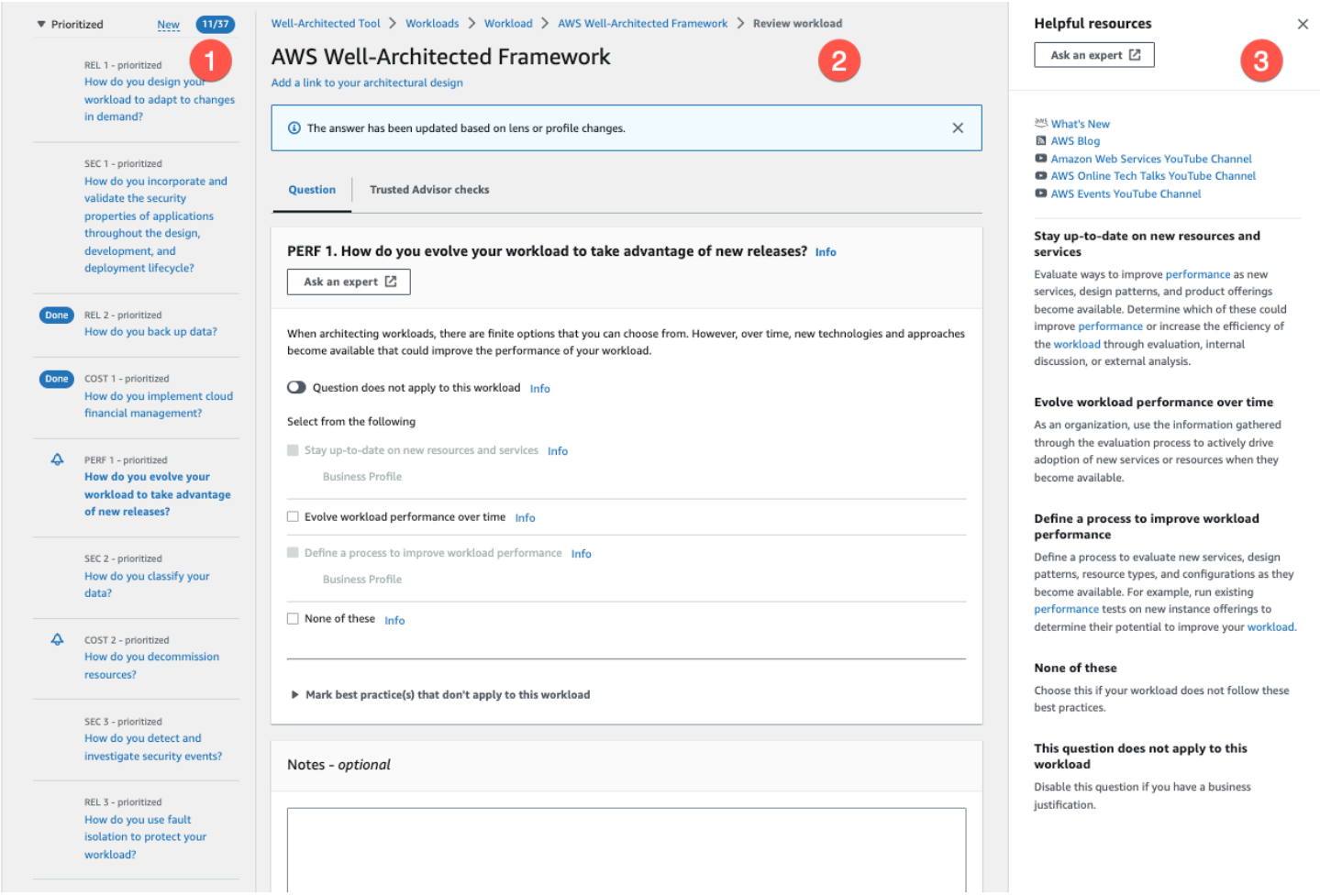
各柱の質問ごとにこれらの手順を繰り返します。

3. 変更を保存し、ワークロードのドキュメント化を一時停止するときは、いつでも [Save and exit (保存して修了)] を選択します。

ワークロードをドキュメント化したら、いつでも質問に戻ってレビューを続行できます。詳細については、「AWS Well-Architected フレームワークを使用したワークロードのレビュー」を参照してください。

# AWS Well-Architected フレームワークを使用したワークロードのレビュー

コンソールの [ワークロードのレビュー] ページでワークロードをレビューできます。このページには、ワークロードのパフォーマンスに関するベストプラクティスと役立つリソースが表示されます。




1. [ワークロードのレビュー] ページを開くには、ワークロードの詳細ページから [レビューを続ける] を選択します。左側のナビゲーションペインには、各柱に関する質問が表示されます。回答した質問には [Done] (完了) と表示されます。各柱の回答された質問の数は柱の名前の横に表示されます。

   他の柱の質問に移動するには、その柱の名前を選択してから回答する質問を選択します。

   (オプション) プロファイルがワークロードに関連付けられている場合は、AWS WA Tool はプロファイル内の情報を使用して、ワークロードレビューのどの質問の優先度が高いか、そしてどの質問がユーザーのビジネスに該当しないのかを判断します。左側のナビゲーションペインで、優

先度が高い質問を使用するとワークロードレビュープロセスを加速できます。優先度の高い質問のリストに新しく追加された質問の横には、通知アイコンが表示されます。

2. 中央のペインには、現在の質問が表示されます。従っているベストプラクティスを選択します。質問に関する詳細やベストプラクティスを入手するには、[Info (情報)] を選択します。[エキスパートに質問する] を選択して、AWS Well-Architected 専用のAWS re:Post コミュニティにアクセスします。AWS re:Post は、AWS フォーラムに代わるトピックベースの質疑応答コミュニティです。re: POST では、回答を検索したり、質問に回答したり、グループに参加したり、人気のトピックをフォローしたり、お気に入りの質問や回答に投票したりできます。

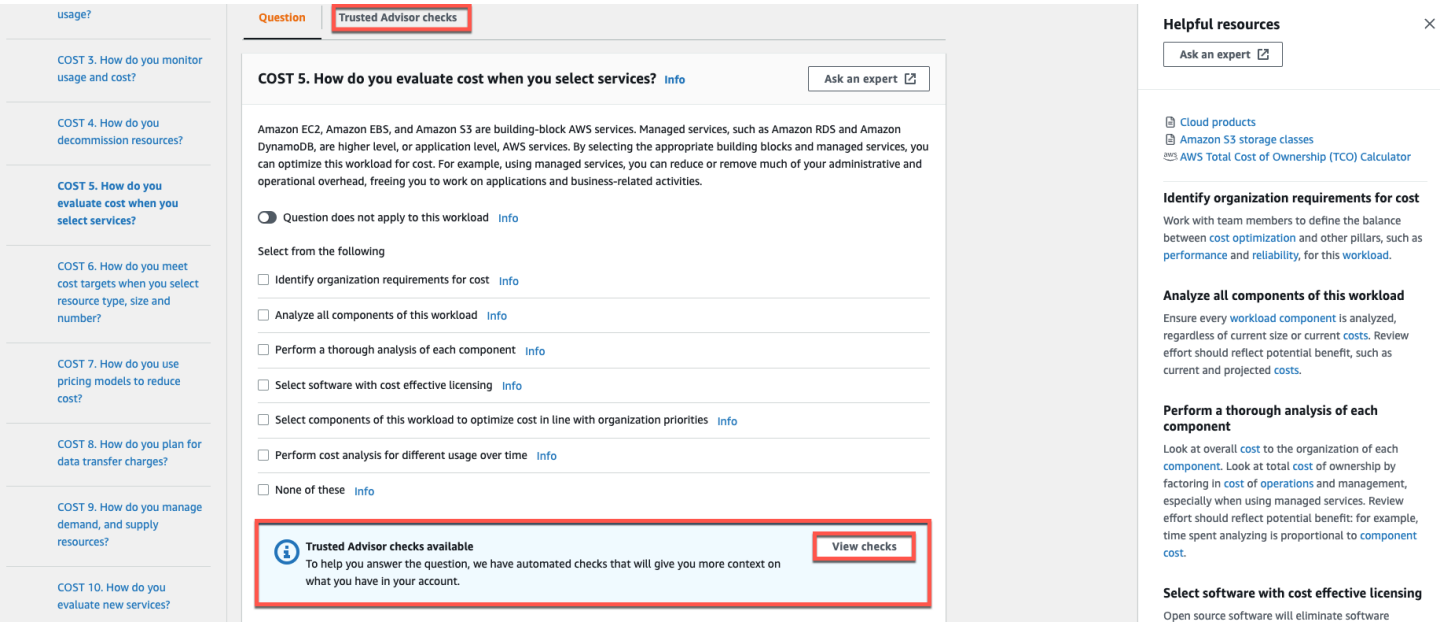
   (オプション) 1 つ以上のベストプラクティスを非適用としてマークするには、[このワークロードに適用されないベストプラクティスをマーク] を選択して、適用されないベストプラクティスを選択します。

   このペインの下部にあるボタンを使用して、次の質問に進むか、前の質問に戻るか、変更内容を保存して終了します。

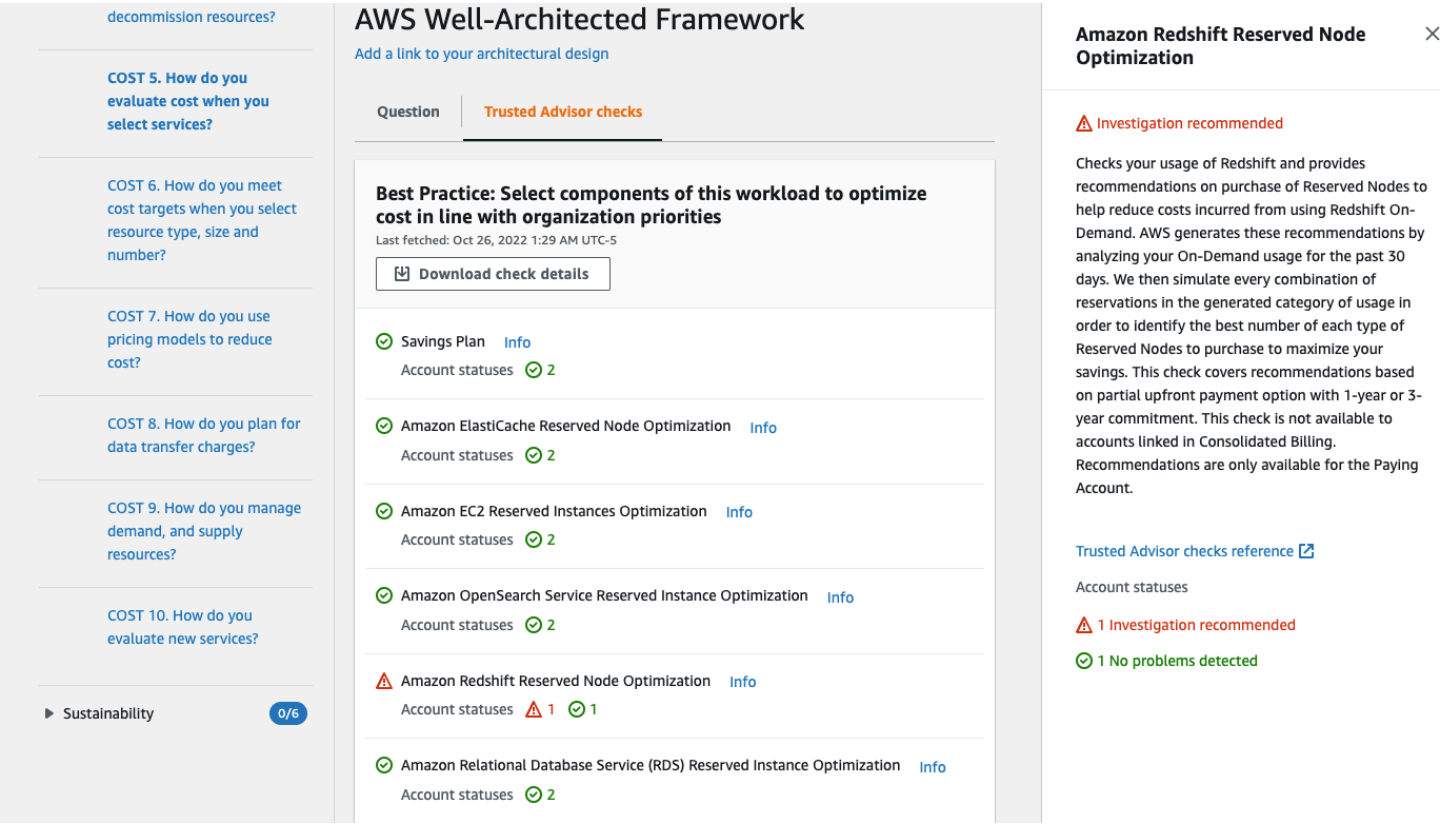
3. 右側のペインに、詳細と役立つリソースが表示されます。[エキスパートに質問する] を選択して、AWS Well-Architected 専用の AWS re: Post コミュニティにアクセスします。このコミュニティでは、AWS のワークロードの設計、構築、デプロイ、運用に関する質問をすることができます。

# ワークロードに対する Trusted Advisor チェックの表示

ワークロードに対して Trusted Advisor が有効化されている場合、[Trusted Advisor のチェック] タブが [質問] の横に表示されます。ベストプラクティスに該当するチェックがある場合は、質問の選択の後に Trusted Advisor のチェックができることを伝える通知が表示されます。[チェックを表示] を選択すると、[Trusted Advisor のチェック] タブに移動します。




[Trusted Advisor のチェック] タブでは、Trusted Advisor のベストプラクティスのチェックに関する詳細情報を確認したり、[ヘルプリソース] ペインの Trusted Advisor ドキュメントへのリンクを表示したり、各ベストプラクティスの Trusted Advisor のチェックやステータスのレポートを CSV ファイルで提供する [チェックの詳細をダウンロードする] を選択したりすることができます。



Trusted Advisor のチェックカテゴリーは色付きのアイコンで表示され、各アイコンの横の数字はそのステータスのアカウント数を示しています。

- [推奨されるアクション (赤色)] – Trusted Advisor は、チェックに対するアクションを推奨します。
- [調査が推奨されるチェック項目 (黄色)] – Trusted Advisor は、チェックの潜在的な問題を検出します。
- [問題は検出されませんでした (緑色)] – Trusted Advisor ではチェックの問題が検出されませんでした。
- [非表示の項目 (グレー)] — チェックで無視するリソースなど、除外項目があるチェックの数。

Trusted Advisor が提供するチェックの詳細については、「サポート ユーザーガイド」の「チェックカテゴリーを表示」を参照してください。

各 Trusted Advisor のチェックの横にある [情報] リンクを選択すると、[ヘルプリソース] ペインにチェックに関する情報が表示されます。詳細については、「サポート ユーザーガイド」の「AWS Trusted Advisor のチェックに関するリファレンス」を参照してください。

# AWS WA Tool でのワークロードのマイルストーンの保存

ワークロードのマイルストーンはいつでも保存できます。マイルストーンには、ワークロードの現在のステータスが記録されます。

マイルストーンを保存するには

1. ワークロード詳細ページで、[Save milestone (マイルストーンの保存)] を選択します。
2. [Milestone name (マイルストーン名)] ボックスに、マイルストーンの名前を入力します。

   > **Note**
   >
   > 名前は 3 ~ 100 文字にします。3 文字以上をスペースにしないでください。ワークロードに関連付けられるマイルストーン名は一意にしてください。一意かどうかを確認するときは、スペースと大文字は無視されます。

3. [保存] を選択します。

マイルストーンを保存した後は、そのマイルストーンに記録されたワークロードデータを変更することはできません。

詳細については、「マイルストーン」を参照してください。

# チュートリアル: AWS Well-Architected Tool ワークロードをドキュメント化する

このチュートリアルでは、AWS Well-Architected Tool を使用してワークロードを文書化および測定する方法について説明します。この例では、小売 e コマースウェブサイトのワークロードを定義してドキュメント化する方法を順を追って説明します。

トピック



## 手順 1: ワークロードを定義する

まず、ワークロードを定義します。ワークロードを定義するには 2 つの方法があります。このチュートリアルでは、レビューテンプレートからワークロードを定義しません。レビューテンプレートからワークロードを定義する方法の詳細については、「the section called “ワークロードの定義”」を参照してください。

ワークロードを定義するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。

   > **Note**
   >
   > ワークロードの状態を文書化するユーザーは、AWS WA Tool への完全なアクセス許可を保持している必要があります。

2. [ワークロードを定義する] セクションで、[ワークロードの定義] を選択します。
3. [名前] ボックスに、ワークロード名として **`Retail Website - North America`** と入力します。
4. [Description (説明)] ボックスに、ワークロードの説明を入力します。

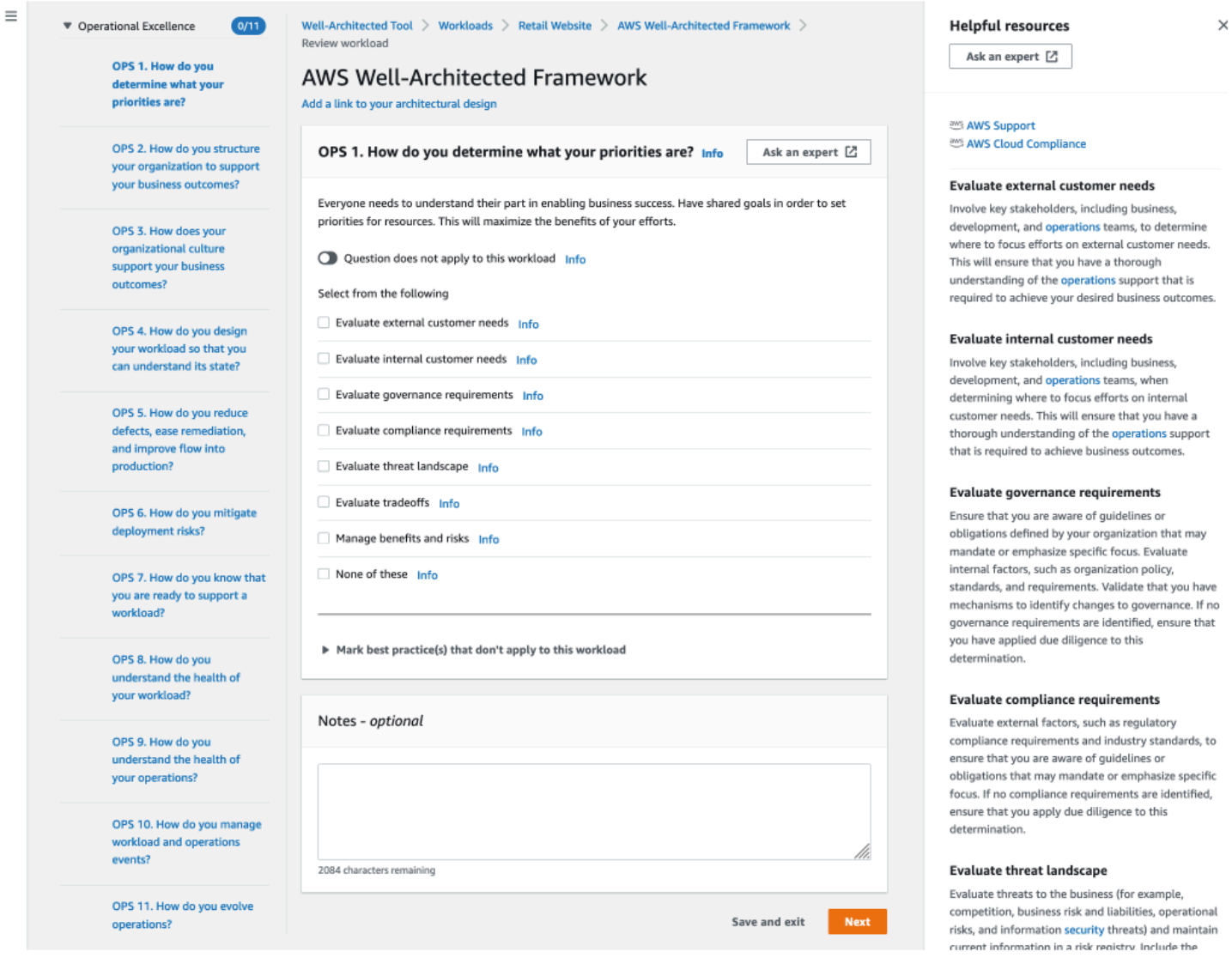
5. [レビューの所有者] ボックスに、ワークロードのレビュープロセスの担当者名を入力します。
6. [環境] ボックスで、ワークロードが本運用環境にあることを示します。
7. ワークロードは AWS とそのローカルデータセンターの両方で実行されます。
   a. [AWS リージョン] を選択し、ワークロードが実行される北米の 2 つのリージョンを選択します。
   b. また、[AWS 以外の領域] を選択して、ローカルデータセンターの名前を入力します。
8. [アカウント ID] ボックスはオプションです。このワークロードには どの AWS アカウント も関連付けないでください。
9. [アプリケーション] ボックスはオプションです。このワークロードにアプリケーション ARN は入力しないでください。
10. [アーキテクチャ図] ボックスはオプションです。このワークロードにアーキテクチャ図を関連付けないでください。
11. [Industry type (産業タイプ)] ボックスと [Industry (産業)] ボックスはオプションで、このワークロードには指定されていません。
12. Trusted Advisor セクションはオプションです。このワークロードに対して、Trusted Advisor サポートを有効化しないでください。
13. Jira セクションはオプションです。このワークロードでは、[Jira] セクションの [アカウントレベルの設定を上書き] をオンにしないでください。
14. この例では、ワークロードにタグを適用していません。[次へ] を選択します。
15. [プロファイルの適用] 手順はオプションです。このワークロードにプロファイルを適用しないでください。[次へ] を選択します。
16. この例では、AWS Well-Architected フレームワークレンズを適用します。このレンズは自動選択されます。[Define workload (ワークロードの定義)] を選択して、これらの値を保存し、ワークロードを定義します。
17. ワークロードを定義したら、[Start reviewing (レビューの開始)] を選択してワークロードの状態のドキュメント化を開始します。

# 手順 2: ワークロードの状態を文書化する

ワークロードの状態を文書化するために、選択したレンズの質問が提示されます。これらは、AWS Well-Architected フレームワークの柱である運用上の優秀性、セキュリティ、信頼性、パフォーマンス効率、コスト最適化およびサステナビリティに関する質問です。

質問ごとに、表示されるリストからお客様が従っているベストプラクティスを選択します。ベストプラクティスに関する詳細が必要な場合は、[Info (情報)] を選択すると、右側のパネルに詳細とリソースが表示されます。

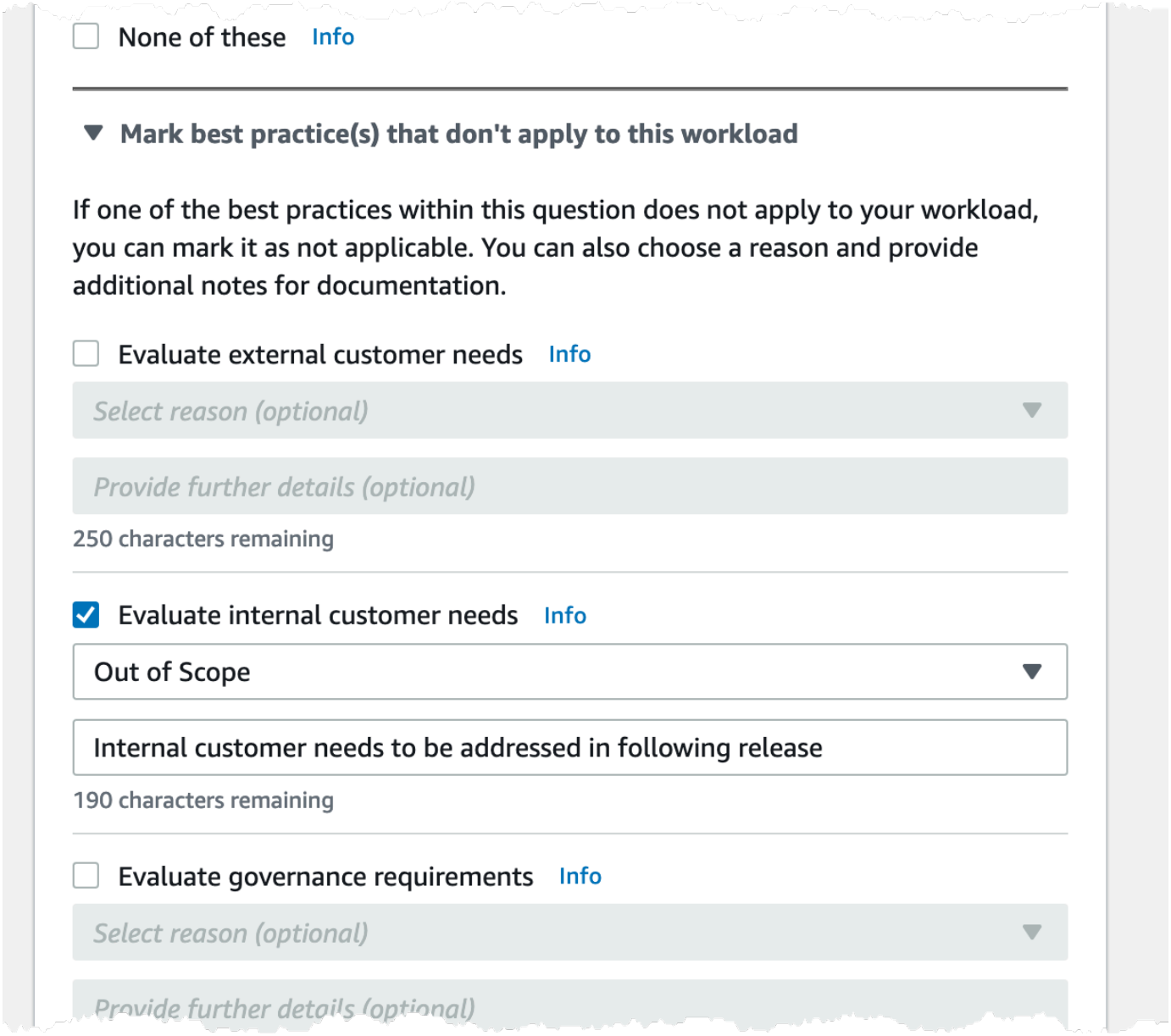
[エキスパートに質問する] を選択して、AWSWell-Architected 専用の AWS re:Post コミュニティにアクセスします。このコミュニティでは、AWS のワークロードの設計、構築、デプロイ、運用に関する質問をすることができます。




1. 次の質問に進むには [Next (次へ)] を選択します。左側のパネルを使用して、同じ柱の別の質問、または別の柱の質問に移動できます。
2. [質問はこのワークロードには該当しません] または [これらのいずれでもない] を選択した場合、AWS は [メモ] ボックスに理由を入力することをお勧めします。これらのコメントはワーク

ロードレポートの一部として含まれ、今後、ワークロードに変更を加えるときに役立つことがあります。

> **Note**
>
> オプションで、1 つ以上の個々のベストプラクティスを適用しないものとしてマークできます。[Mark best practice(s) that don't apply to this workload] (このワークロードに適用されないベストプラクティスをマーク) を選択し、適用されないベストプラクティスを選択します。オプションで理由を選択し、追加の詳細を入力できます。適用されないベストプラクティスごとにこれを繰り返します。




> **Note**
>
> このプロセスは [保存して終了] を選択していつでも一時停止できます。後で再開するには、AWS WA Tool コンソールを開いて左側のナビゲーションペインで [ワークロード] を選択します。

3. ワークロードの名前を選択して、ワークロードの詳細ページを開きます。
4. [Continue reviewing (レビューを続ける)] を選択すると、中断した場所に移動します。

5. すべての質問を完了すると、ワークロードの概要ページが表示されます。今すぐこれらの詳細をレビューできます。または、後で左側のナビゲーションペインで [Workloads (ワークロード)] を選択し、ワークロード名を選択して詳細に移動できます。

ワークロードの状態を初めてドキュメント化した後、マイルストーンを保存してワークロードレポートを生成する必要があります。

マイルストーンにはワークロードの現在の状態が記録されるため、改善計画に基づいて変更を加えながら進捗状況を評価できます。

[ワークロードの詳細] ページから:

1. [ワークロードの概要] セクションで、[マイルストーンを保存] ボタンを選択します。
2. マイルストーン名として **`Version 1.0 - initial review`** と入力します。
3. [保存] を選択します。
4. ワークロードレポートを生成するには、目的のレンズを選択します。[Generate report (レポートの生成)] を選択すると、PDF ファイルが作成されます。このファイルには、ワークロードの状態、特定されたリスクの数、推奨される改善点のリストが含まれています。

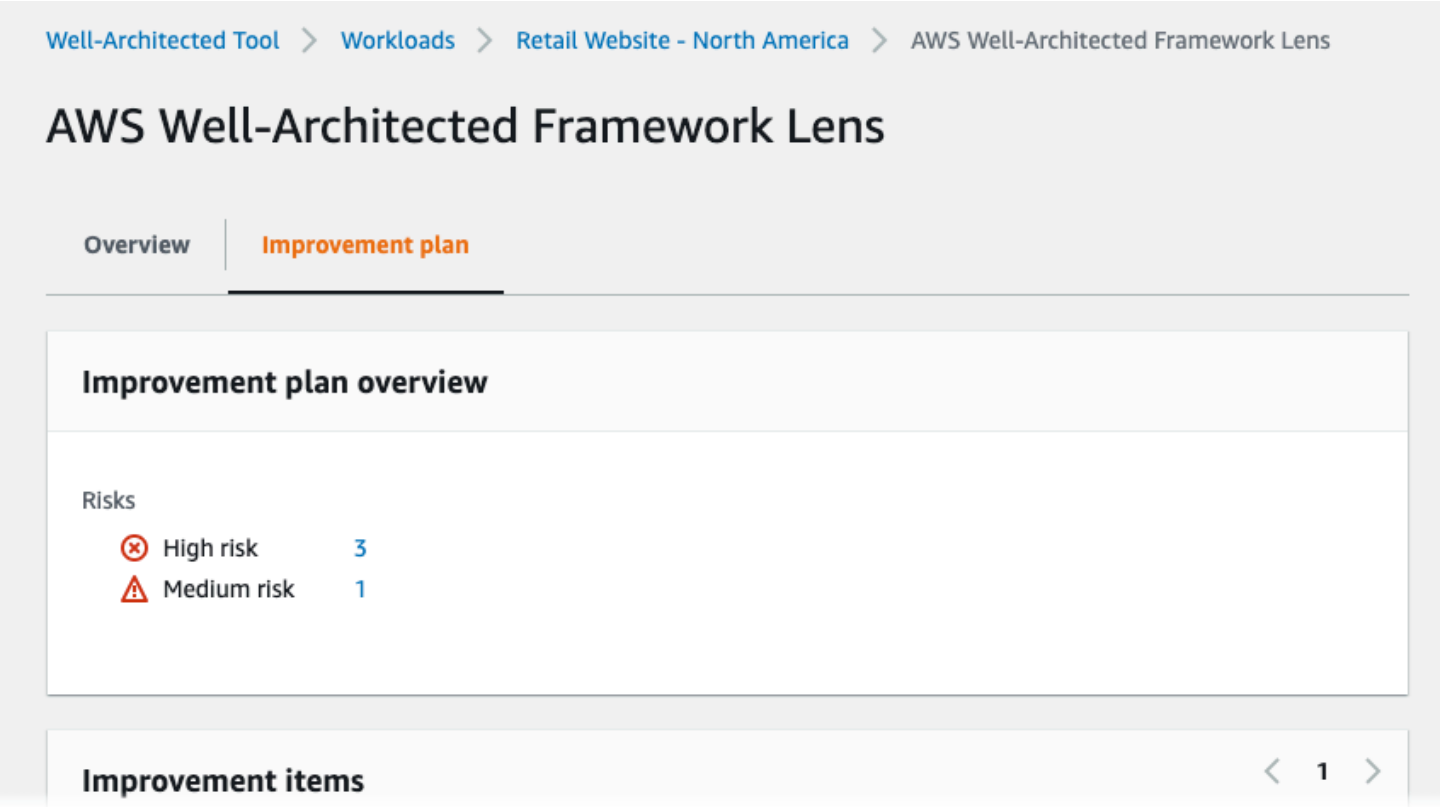
# 手順 3: 改善計画をレビューする

選択したベストプラクティスに基づいて、AWS WA Tool は、AWS Well-Architected フレームワークレンズに対して評価された高リスクおよび中リスクの領域を特定します。

改善計画をレビューするには:

1. [概要] ページの [レンズ] セクションで、[AWS Well-Architected フレームワーク] を選択します。
2. 次に、[Improvement plan (改善計画)] を選択します。

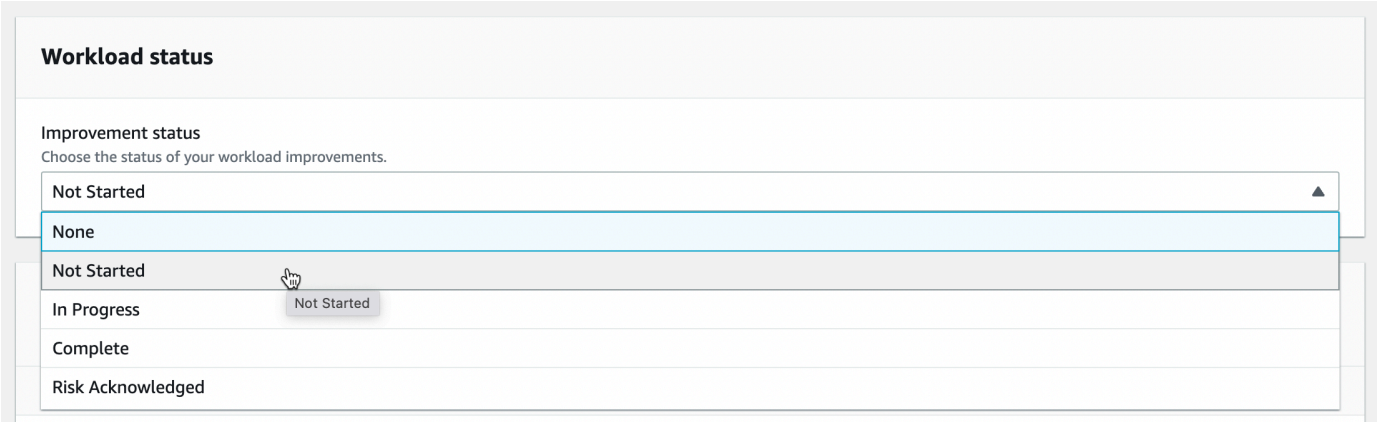
このワークロードの例では、AWS Well-Architected フレームワークレンズによって高リスクと中リスクの問題が特定されています。




ワークロードの[改善ステータス]を更新して、ワークロードへの改善がまだ開始されていないことを周知します。

[改善ステータス] を変更するには:

1. 改善計画から、ページ上部のパンくずリストにあるワークロードの名前 (**`Retail Website - North America`**) をクリックします。
2. [プロパティ] タブをクリックします。
3. [ワークロードのステータス] セクションに移動し、ドロップダウンリストで [未開始] を選択します。



4. [概要] タブをクリックして [プロパティ] タブに戻り、[レンズ] セクションの AWS Well-Architected フレームワークリンクをクリックします。次に、ページ上部の [改善計画] タブをクリックします。

[Improvement items (改善項目)] セクションには、ワークロードで特定された推奨改善項目が表示されます。質問は、設定した優先度に基づいて並べ替えられ、まず高リスクの問題が、次に中リスクの問題が表示されます。

質問のベストプラクティスを表示するには、[Recommended improvement items (推奨改善項目)] を展開します。推奨改善アクションはそれぞれ、特定されたリスクを排除するか少なくとも軽減するのに役立つ、エキスパートからの詳細なガイダンスにリンクされています。

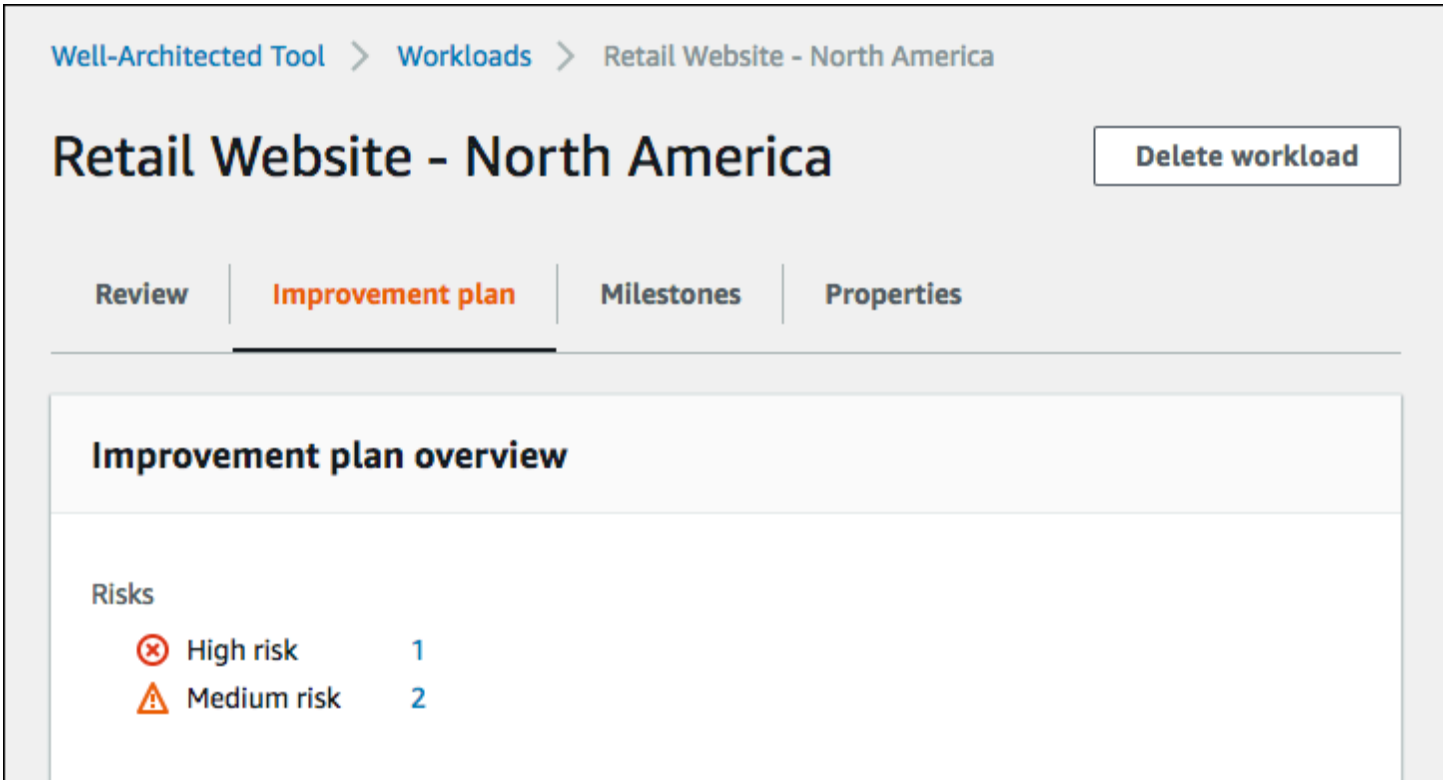
プロファイルがワークロードに関連付けられている場合は、優先度の高いリスクの数が [改善計画の概要] セクションに表示され、[プロファイルによる優先度] を選択することで [改善項目] のリストをフィルタできます。改善項目のリストには、[優先度] ラベルが表示されます。

# 手順 4: 改善を行って進捗を評価する

改善計画の一環としてワークロードに Amazon CloudWatch と AWS Auto Scaling のサポートを追加することで、高リスクの問題の 1 つに対処しました。

[改善項目] セクションから:

1. 関連のある質問を選択し、変更を反映するように選択したベストプラクティスを更新します。改善点を記録するメモが追加されます。
2. 次に [保存して終了] を選択してワークロードの状態を更新します。
3. 変更を加えた後は [Improvement plan (改善計画)] に戻り、それらの変更がワークロードに与えた影響を確認できます。この例では、これらのアクションによりリスクプロファイルが改善され、高リスクの問題が 3 つから 1 つに減少しました。




この時点でマイルストーンを保存してから [Milestones (マイルストーン)] に移動し、ワークロードがどのように改善されたかを確認できます。

# Well-Architected フレームワークレビュー (WAFR)

Well-Architected フレームワークは、クラウドでワークロードを作成および実行するための主要な概念と設計原則について説明しています。AWS でシステムを構築する際に行う決定の長所と短所を理解するのに役立ちます。フレームワークを利用することで、信頼性、安全性、効率性、コスト効率、持続可能性に優れたアプリケーションを設計および運用するためのアーキテクチャに関するベストプラクティスを学ぶことができます。

Well-Architected フレームワークレビュー (WAFR) では、一連の基本的な質問に回答して、アーキテクチャがクラウドのベストプラクティスとどの程度一致しているかを学習し、改善を実施するためのガイダンスを受け取ります。

## WAFR フェーズ

WAFR プロセスは 3 つの主要なフェーズで構成されます。

- 準備: 適切な計画とステークホルダーの調整を行い、成功に向けてセットアップする
- レビュー: AWS ベストプラクティスに照らして実際の評価を実施する
- 改善: 検出結果をワークロードの実行可能な改善に変える

このドキュメントでは、3 つのフェーズについて説明し、レビューフェーズから最大の価値を引き出すための十分な準備が整っていることを確認します。また、WAFR の検出結果をワークロードの実行可能な改善に変える方法についても説明します。

## WAFR の準備

十分な準備をせずに Well-Architected フレームワークレビュー (WAFR) を急いで実行しないことが重要です。急ぐと、プロセスが予想よりも長くかかることになり、好ましくない結果をもたらし、行動を起こすことがより困難になります。

アーキテクチャのレビューには、人的コストが伴います。グループまたはチームメンバーが事前に準備できれば、セッションに参加するためにより多くの人を必要とする後の段階で時間を節約できます。これにより、セッション計画の改善と非同期通信手法により、大規模なグループディスカッションの必要性も排除できます。

ワークロードの所有者、設計方法、目的、組織のビジネス成果との整合性を明確に定義することで、レビューフェーズと改善フェーズでより良い結果を達成できます。

準備フェーズは、次の 3 つの主要な要素で構成されます。

1. ワークロードとスコープ
2. 人と文化
3. ドキュメントとインフラストラクチャ

# ワークロードとスコープ

AWS Well-Architected フレームワークによると:

> ワークロードは、リソースと、ビジネス価値をもたらすコード (顧客向けアプリケーションやバックエンドプロセスなど) の集まりです。ワークロードは、1 つの AWS アカウント内のリソースのサブセットで構成されている場合もあれば、複数の AWS アカウントにまたがる複数のリソースの集合になっている場合もあります。中小企業では、ほんの数ワークロードになる一方、大企業では、数千ワークロードにもなることがあります。

ワークロードは、クラウドサービスやリソース以上のものです。また、人、チーム、プロセス、ランブック、ビジネス価値を提供するテクノロジーとインフラストラクチャも含まれます。WAFR を実行する前に、ワークロードのコンポーネントを理解して文書化するために時間を費やしてください。これにより、レビューフェーズの時間を節約できます。

## WAFR のワークロードの選択

WAFR のワークロードを準備するには、チームと以下の質問について話し合います。

- ワークロードの所有者は誰ですか? ワークロードの中断がビジネスに影響を与える場合、誰が責任を負いますか?
- ワークロードの目的は何ですか? ビジネスに関する分析はありますか? サンドボックス、トレーニング、ログ記録はありますか?
- このワークロードは存在する必要がありますか? シャットダウンするとどうなりますか?
- ワークロードは顧客向けですか、それとも社内向けですか?
- ワークロードは本番稼働用ですか、非本番稼働用ですか?
- ライフサイクルのワークロードはどのフェーズですか?
- ワークロードが中断した場合の影響は何ですか?
- ワークロードの境界はどこまでですか?
- このワークロードにはどのような依存関係がありますか?

WAFR を続行する前にワークロードを評価するときに、これらの質問のほとんどに明確に回答できる必要があります。

### レビューの範囲はどの程度ですか

最終的に WAFR はフレームワークのすべての柱にまたがりますが、意思決定を行う前にトレードオフを特定し、コンテキストを理解できます。開始する良い方法は、優先順位の高い柱またはワークロードの特定領域に焦点を当てることです。

より大きなレビュープロセスを定義し、実行可能な結果を生成し、反復することで、ワークロードとビジネスにより多くの価値を生み出すことができます。

段階的なアプローチを検討してください。

1. 現在のビジネスおよび技術コンテキストに最も関連性の高い主要な柱を 2～3 つ特定する
2. これらの柱内のワークロードの価値を示す
3. 十分な結果が得られたら、さらに多くの柱で繰り返す

スコープをさらに減らすには、ワークロード専用に設計されたレンズを使用します。

## 人と文化

すべてのワークロードには所有者が必要であり、多くの人やチームがワークロードのライフサイクルに関与している可能性があります。ただし、WAFR を実行する前に、ワークロードのシングルスレッドオーナー (STO) を定義します。

この担当者は、意思決定を行い、予算、人員、ロードマップを管理できる必要があります。このロールの例は、プロダクトオーナー、プロダクトマネージャー、ヘッドアーキテクト、またはエンジニアリングマネージャーです。

最終的に、ワークロードが意図したとおりに機能しなくなった場合、このロールが責任を負います。

成果を向上させるには、STO と共に WAFR を実行することが重要です。例えば、ワークロードの改善項目が見つかったものの、製品ロードマップで優先順位を付けがうまくいかない場合があります。または、作業を実行するための資金やリソースの取得に苦労することがあります。

これは多くの場合、達成不可能なバックログ項目のリストを収集する結果となります。STO は、WAFR を所有し、プロセスに投資しているため、この結果を回避するのに役立ちます。

## 必要なステークホルダー

STO はすべての質問に答えることはできません。多くの人々やチームが、ワークロードの設計、開発、保護、運用に関与しています。ワークロードの組織とサイズに応じて、関係するステークホルダーとチームの数は異なります。

ステークホルダーに関する以下の質問を検討してください。

1. 質問の各カテゴリに回答するために、誰が出席する必要がありますか?
2. WAFR のどの部分にどのステークホルダーが出席する必要がありますか?
3. さまざまなステークホルダーに質問について事前に通知するにはどうすればよいですか?

## 柱スポンサー

Well-Architected フレームワークは 6 つの柱で構成されています。STO の定義は重要ですが、WAFR プロセスの価値を加速および向上させるには、柱固有のスポンサーや推進者からサポートを集めることが重要です。

以下のことができる柱のスポンサーまたは推進者を定義します。

- WAFR の特定部分に参加して情報またはガイダンスを提供する
- 対象領域の結果を所有する
- 組織間の戦略的変更を定義、影響、伝達する

組織には Cloud Center of Excellence または Cloud Community of Practice がありますか? 小規模から始めて、アーキテクチャの健全性に関する議論と改善でお互いをサポートできる同じ考え方の人々のグループを増やします。

## 安全なスペースを作成する

テクノロジーの選択に関する健全で生産的な議論を行うには、健全な組織文化を育むことが不可欠です。WAFR に関与する人々のグループには、ワークロードに新しい人または古い人、在職期間や年功の異なる人、パートナーや第三者として関与しているもいます。永続的で有用な改善の可能性を向上させるには、ワークロードについて健全で敬意のある対話を育むことが重要です。

最初からポジティブな意図を設定し、全体で再度強調して整合性を維持し、改善の機会の発見に集中します。テクノロジーとベストプラクティスは進化するため、WAFR は改善点を発見する機会として捉える必要があります。

WAFR は監査ではありません。結果はさまざまなコンプライアンス基準を満たすのに役立ちますが、ワークロードを「スコア化」するプロセスは存在しません。アーキテクチャの健全性の向上に焦点を当てます。

WAFR は「私たちはどこにいるのか」と問いかけ、ワークロードの特定の時点でのビューをキャプチャする機会です。その後、検出結果を使用して、情報に基づいた意思決定を行い、「どこへ行くべきか」という問いに答えることができます。

アーキテクチャの改善は、AWS Well-Architected がガイドするジャーニーです。WAFR プロセスを開始するときは、次の質問を考慮してください。

1. WAFR を実行する理由は何ですか?
2. そこから何を得たいですか?
3. エクスペリエンスは全員にどのようなメリットをもたらしますか?
4. 現在どこにいて、どこに行きたいですか?

### リソース

- Accountability Blog Post
- Amazon Two Pizza Teams

## ドキュメントとインフラストラクチャ

WAFR を実行すると、従うべきベストプラクティスの多くについて、文書化されたプロセス、標準運用手順 (SOP)、ランブック、プレイブックがあることがわかります。WAFR 中に、Well-Architected Tool (WA ツール) 内のメモフィールドに情報とコンテキストを記録します。ワークロードに関連するすべての関連ドキュメントアーティファクトを事前に収集することで、レビュー中の時間を節約できます。

ドキュメントを検討するときは、次の質問を考慮してください。

- ワークロードに関するドキュメントにはどのようなものがありますか?
- どのドキュメントが欠落していますか?
- これらのアーティファクトを作成および保存するには、どのようなツールを使用しますか?

- これらのアーティファクトの作成とメンテナンスには誰が関与しますか?

ワークロードに関するドキュメントの例を以下に示します。

- ワークロード Wiki ページ
- アーキテクチャ図
- アーキテクチャ決定レコード (ADR)
- 標準操作手順 (SOP)
- Infrastructure as Code (IaC) リポジトリ
- ネットワークトポロジ
- プレイブックとランブック
- 組織またはチームの構造
- マルチアカウント戦略ドキュメント
- 中央 ID プロバイダーの設定
- 中央モニタリングソリューションの設定
- 依存ワークロードのドキュメント
- API リファレンスガイド
- ソフトウェアライブラリのバージョン
- エラー修正 (COE) プロセスと履歴
- カオスエンジニアリング戦略
- ロードテストチームの詳細
- 脅威モデル
- チームレトロスペクティブ
- ゲームデーのドキュメント

## アンチパターン

これらのリソースが存在しない場合でも、検出メカニズムとして WAFR を実行できます。ただし、これらのアーティファクトがないと、プロセスに時間がかかる場合があります。ドキュメントアセットの作成は、アーキテクチャの健全性向上に向けた最初のステップとなります。

## ワークロードの検出

コンポーネントやリソースを知らずに、アーキテクチャを効率的にレビューすることは困難です。レガシーワークロードは、時間の経過とともに進化したり、所有権が変更されたりすることが多

く、AWS CloudFormation、AWS CDK、Terraform などの Infrastructure as Code (IaC) ツールを使用して定義されていない可能性があります。

改善点について説明する前に、ワークロードのさまざまなアーキテクチャコンポーネントとその依存関係を理解し、共通の理解を提供するための視覚的表現を作成します。

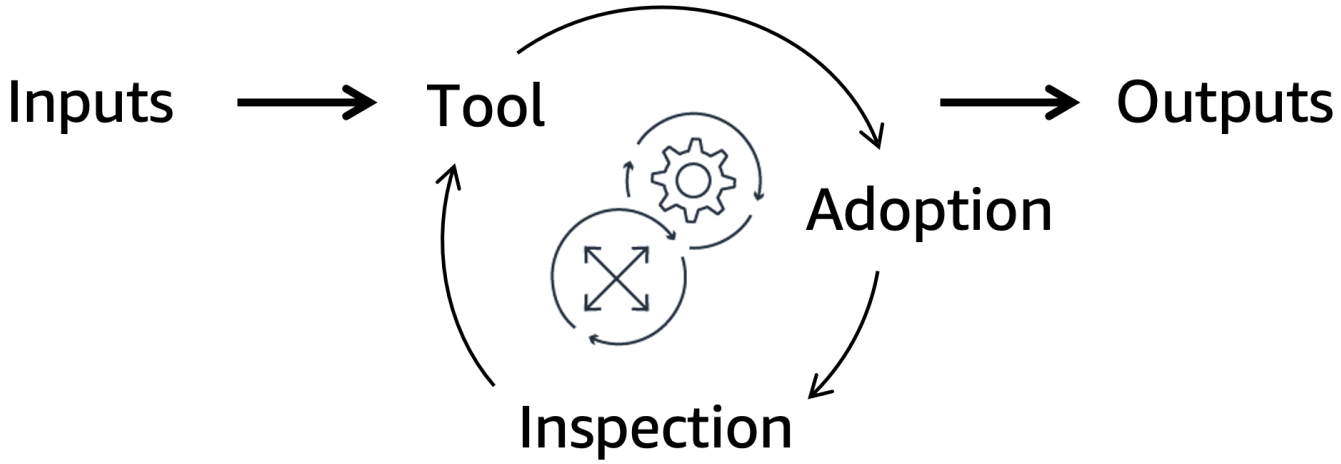
ソフトウェアベンダーから直接、AWS Marketplace から、またはオープンソースソリューションとして入手できるサードパーティーの検出および自動ダイアグラム作成ツールは多数あります。

### リソース

- AWS リファレンスアーキテクチャ図
- Architectural Decision Record Process
- ADR GitHub Home
- correction of error (COE) を開発すべき理由
- Workload Discovery On AWS Solution

## メカニズム

メカニズムは、人間の最善の努力を、多くの場合自動化された反復可能でスケーラブルなプロセスやツールに置き換え、望ましい成果を達成します。メカニズムは、ツールまたはプロセスを作成し、その採用を推進し、結果を検査して軌道修正する完全なサイクルです。このサイクルでは、制御可能な入力を取得し、継続的な出力に変換して、繰り返し発生するビジネス課題に対処します。




メカニズムの周期的な性質は、繰り返し発生する問題や機会の解決に最適です。WAFR は、ツール、導入プロセス、検査プロセスを備えたメカニズムであり、すべてが完全なサイクルで動作します。

ワークロードの WAFR を実施すると、組織内で他のメカニズムを開発するための改善の機会を特定できます。WAFR の結果は、1 つのチームに対する 1 回限りの修正ではなく、複数のチーム間で共有される必要があり、それによって最大限の価値を実現できます。

## ビジネス上の成果

テクノロジーに変更を加える前に、ビジネスの優先順位を決定します。組織の優先順位を明確に理解せずにアーキテクチャをレビューするのはあまり効果的ではありません。これらの優先順位は、整合性を維持し、より良い結果をもたらすためのガイドラインとして役立ちます。

ビジネス成果は、組織戦略に結び付けられ、顧客のフィードバックによって推進される重要な価値の高いビジネス目標です。これらは意図的に高レベルであるため、さまざまなチームがそれらの成果を達成するためにより具体的な目標を定義できます。

一般的なビジネス成果の例は次のとおりです。

- コストの削減
- 利益の増加
- 顧客満足度の向上
- 顧客保持率の向上
- スタッフの保持率の向上
- 環境の持続可能性の向上
- セキュリティ態勢の強化

組織のビジネス成果を認識し、そこから逆算して作業を進めることで、組織の目標達成に最も大きな影響を与える可能性のあるテクノロジーの変化に重点を置き、時間を節約できます。これにより、リーダーシップに対する信頼が高まります。

組織、ビジネスユニット、またはチームの現在のビジネス上の優先事項を見つけて話し合います。

## リソース

- How to perform a Well-Architected Framework Review - Part 1

# WAFR の実行

必要な準備がすべて完了したら、Well-Architected フレームワークレビュー (WAFR) を実行します。このセクションでは、WAFR の実施をより効率的にするためのヒントとコツについて説明します。

# WAFR の前に

ワークロードをグループとして議論する前に、次のセクションに進み、セッションのエンゲージメントルールについて話し合います。続行する方法については、グループ内でコンセンサスが必要です。

### 役割と責任を定義する:

- WAFR を主導するのは誰ですか?
- 誰が画面を共有し、何を共有しますか?
- WA ツールまたは別の形式でメモを取るのは誰ですか?
- どの柱をどの順序で確認しますか?
- 質問に答える適切な人材が部屋にいますか?
- 範囲外の項目をどのようにキャプチャし、これらの項目のバックログをどのように作成しますか?
- 各セクションまたは柱にどれくらいの時間を割り当てますか?
- 割り当てられた時間内で何を達成したいですか?

# レビューのヒント

ワークロードアーキテクチャの選択に関するデータポイントをキャプチャすることを中心に会議を計画します。WAFR のこのセクションをできるだけスムーズにするためにできることがいくつかあります。

1. 肯定的な意図を伝える: WAFR の肯定的な意図を参加者と再確認します。仕事に関する重要な会話は難しい場合があるため、WAFR が改善の機会を見つけるために実施されていることを再確認してください。非難しない文化を強化します。攻撃も防御もなく、アーキテクチャの改善について協力して議論します。
2. サポーターを取り込む: 複雑なワークロードアーキテクチャをナビゲートし、質問し、応答を調整し、メモを取ることは、1 人で実行するには難しい場合があります。WAFR の成功はチームアクティビティです。代わりの役割を指定して、あるユーザーがレビューを実行し、別のユーザーがメモを取り、ドキュメントを確認し、ディスカッションを監視できるようにします。
3. トピックに留まる: アーキテクチャ上の決定についてグループで会話するときに、人々が脱線してしまうことはよくあります。時間を効率よく使いたい場合は、WAFR 参加者が互いに尊重し合ってトピックに留まるようにしてください。サイドコンセプトとアイデアを一元化された場所に記録し、今後のディスカッションセッションで取り上げることができます。
4. 適切なメモを取る: WA ツールのボックスにチェックを入れるだけでは、後のマイルストーンで WAFR を再検討する人にコンテキストが提供されません。WA ツールのメモボックスを使用するか、文字制限を超えた場合は WAFR メモボックスからリンクされた外部ドキュメントを作成しま

す。コンテキストは、他の関係者、特にワークロードを初めて使用する人が進行中の作業を理解し、優先順位を決定するのに役立ちます。

5. ソリューションに焦点を当てない: ソリューションではなく、ワークロードに関するデータポイントのキャプチャに焦点を当てます。ソリューションに重点を置きすぎると、WAFR セッション中に時間が浪費され、重要なデータポイントを取得できなくなる可能性があります。範囲外のことをブレインストーミングするのは、他の参加者の時間を最大限に活用することにはなりません。
6. ツールではなくワークロードに焦点を当てる: AWS マネジメントコンソールの Well-Architected Tool (WA ツール) を表示した画面を共有するのは一般的です。WA ツールでデータをキャプチャすることは重要ですが、ツールだけに集中しないでください。代わりに、アーキテクチャに関するディスカッションに焦点を当ててください。レビューは会話形式にし、コンテキストに合わせて質問を言い換えます。
7. ディスカッションをパートに分割する: 1 回の会議で 6 つの柱をすべて確認するのは難しい場合があります。レビューを小さなセッションに分割することで、トピックをターゲットにしたアプローチが可能になり、参加者とのスケジューリングが容易になります。
8. 休憩を取ることを忘れない: アーキテクチャを徹底的に確認することは参加者にとって疲れる可能性があり、時間の経過とともに集中力が低下する可能性があります。WAFR 中は頻繁に休憩をスケジュールします。参加者の時間を大切にし、必要がなくなった時点で退席できるようにします。
9. 可能性について慎重に考える: 質問に対する答えが、「たぶん」、「そのような」、「対処するための何かがバックログにあります」である場合は、それが実質的に「いいえ」を意味していないか慎重に検討してください。WAFR とは、意図した状態ではなく、ワークロードの正直な現在の状態をキャプチャすることを目的としています。
10. トレードオフを検討する: Well-Architected は各柱間でトレードオフを行うことに重点を置いています。ワークロードの耐障害性を高めるとコスト最適化が損なわれる可能性があり、またコストをさらに最適化するとワークロードの環境への影響が悪化する可能性があります。柱は、会話の枠組みを提供し、情報に基づいたアーキテクチャの選択を行うのに役立ちます。
11. 完璧なワークロードは存在しないことを認識する: ワークロードが完璧であることは稀で、完璧である必要もほとんどありません。WAFR を完璧主義の追求とすることを避け、ワークロードが意図されたビジネス目的に沿って安全かつ効率的に機能することに重点を置いてください。

## WAFR の実行

AWS アカウントでワークロードと並行して WAFR を実行します。その後、ワークロードレビューを他の AWS アカウントと共有できます。

AWS Organizations を使用して、中央アカウントとレビューを共有します。その後、ダッシュボードを使用して組織のワークロードを一元的に表示できます。

これにより、すべてのワークロードにおけるリスクと改善のパターンを認識できます。その後、多くのアカウントやワークロードで共有して使用できるパターンベースのアプローチで、課題に一元的に対処できます。

## IAM アクセス

AWS WA Tool でAWS マネジメントコンソールにアクセスするには、IAM アクセス許可が必要です。WAFR セッションの開始時に時間を節約するために、事前にアクセスが必要なユーザーを決定します。

詳細については、「ユーザー、グループ、ロールに AWS Well-Architected Tool へのアクセスを提供する」を参照してください。

クロスアカウント IAM ロールを設定して、外部ステークホルダーが WA ツールにアクセスし、レビューを編集または表示できるようにします。

## リソース

- How to perform a Well-Architected Framework Review Part 2

# ワークロードの改善

この時点で、WAFR の準備をし、レビューを完了し、AWS ベストプラクティスに照らしてワークロードを評価しました。

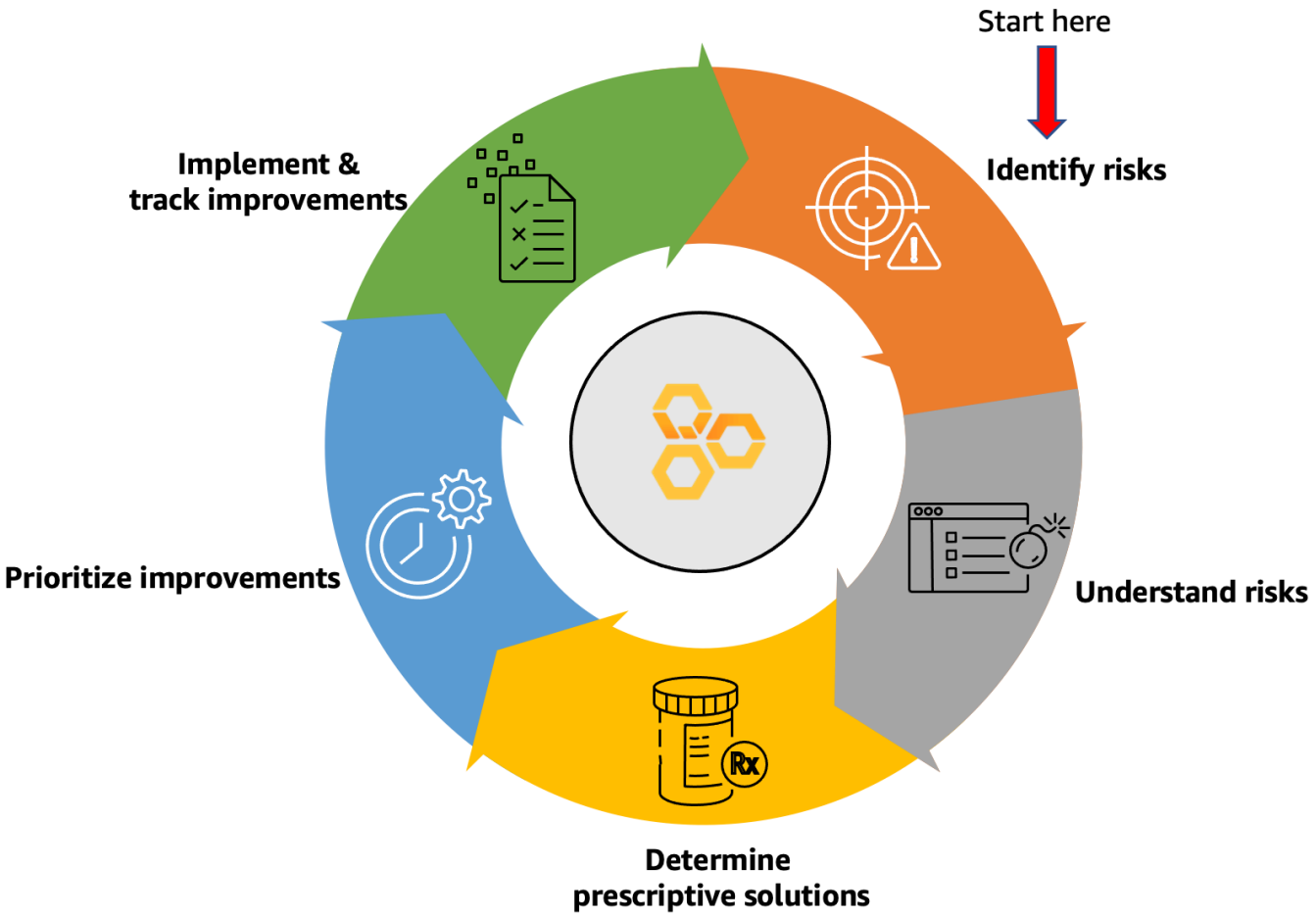
WAFR からの出力では、レビュー中にキャプチャされた回答に基づいてアーキテクチャ上のリスクが特定されます。これらのリスクは、高リスク問題 (HRI) と中リスク問題 (MRI) に分類されます。

最後のフェーズでは、リスクのリストを作成し、ビジネスへの影響を理解し、ソリューションを特定し、組織の優先順位に従ってそれらのソリューションを実装する改善計画を作成します。

以下のセクションでは、ワークロードの改善プロセスに関する詳細なガイダンスを提供します。

- リスクを特定して理解する
- 規範的ソリューションを決定する
- 改善の優先順位付け
- 改善の実装と追跡

次のサイクルは、WAFR の改善フェーズに含まれる主なステップを示しています。




## リスクを特定して理解する

特定されたリスクを改善の機会と見なします。

WAFR のコンテキストにおけるリスクには、高リスク問題 (HRI) と中リスク問題 (MRI) の 2 つのカテゴリがあります。

- 高リスクの問題 (HRI): ビジネスに重大な悪影響を及ぼす可能性がある、アーキテクチャおよび運用上の選択肢です。高リスクのベストプラクティスは、柱内の基本的な必須のプラクティスと見なされます。これらは、組織の運用、アセット、個人に影響を与える可能性があります。セキュリティの柱における HRI の例としては、AWS アカウントを保護していないことが挙げられます。
- 中リスクの問題 (MRI): ビジネスに悪影響を及ぼす可能性もあるが、HRI よりも程度は低い選択肢。中リスクのベストプラクティスは、ワークロードを大幅に改善できる有効な手法を表します。セキュリティの柱に関する MRI の例は、認証情報を定期的に監査およびローテーションしないことです。

## レポートの生成

HRI と MRI を視覚的に識別する最初のステップは、レビューした各ワークロードのリスクを示すレポートを生成することです。

AWS Well-Architected Tool (AWS WA ツール) ダッシュボードは、ワークロード、および関連する HRI と MRI へのアクセスを提供します。自分と共有されているワークロードを含めることもできます。ダッシュボードを使用すると、ワークロード、柱、重要度 (高または中) で問題をフィルタリングできます。

ダッシュボードページには、柱または重要度でフィルタリングされた HRI と MRI のリストが表示されます。改善項目を選択すると、Well-Architected フレームワークからそれに関連するベストプラクティスに直接移動します。そこから、問題を修正するために必要な推奨アクションと必要なリソースを確認できます。

WA ツールダッシュボードから [レポートの生成] を選択すると、これらのすべての検出結果を 1 つのレポートにまとめることができます。

要約メールをレポートとともに WAFR 参加者に送信し、主要な検出結果と推奨される改善計画を要約して次のステップに備えることをお勧めします。

## リスクの管理

リスクを効果的に管理するには、リスクとその許容レベルを定義することが重要です。リスク分析では、潜在的な問題とは何か、それらが問題であるかどうかを知る方法について説明します。

リスク評価を実行するには、主に 2 つの方法があります。

- 定量的: 加重目標データを使用して、コスト超過、リソース消費、スケジュール遅延の観点からリスクの影響を評価します。
- 定性的: コストまたは利点の実際の値に関連しない主観的なデータを使用して、確率と全体的な影響を測定します。

場合によっては、両方のアプローチの長所をマージしてリスクの影響を評価するハイブリッドアプローチを使用することがあります。

HRI と MRI 定義に基づいてリスクのレベルを評価するときは、次の質問を検討してください。

- リスクが影響をもたらす可能性はどれくらいですか?
- 顧客にはどのような影響がありますか?

- その結果、ビジネスにどのような影響がありますか?
- リスクは完全に除去できますか、あるいは軽減することしかできませんか?
- リスクを負うのは誰ですか?
- 除去または軽減のための改善作業の所有者は誰ですか?
- この結果が再び発生する確率はどれくらいですか? 同じ影響を与える可能性がありますか?
- 結果の可能性と再発パターンの関係を特定できますか?

主要なステークホルダーまたはビジネスオーナーにこれらの質問に答えてもらうことは、焦点を当てる最も重要なリスクのリストと、それらに対処するための予測時間を作成するのに役立ちます。

### リスクの大きさ

次の表は、リスクの大きさを判断するのに役立ちます。

| 可能性 x 影響 | ごくわずか (1) | 軽微 (2) | 中 (3) | 重要 (4) | 非常事態 (5) |
|---|---|---|---|---|---|
| ほぼ確実 (5) | 5 | 10 | 15 | 20 | 25 |
| 可能性あり (4) | 4 | 8 | 12 | 26 | 20 |
| 可能 (3) | 3 | 6 | 9 | 12 | 15 |
| 可能性が低い (2) | 2 | 4 | 6 | 8 | 10 |
| まれ (1) | 1 | 2 | 3 | 4 | 5 |

HRI と MRI およびそれらがビジネスにもたらすリスクについてグループとして取り組みます。対処する必要がある HRI のリストを作成します。ビジネスの重要度に基づいてリスクをランク付けし、優先順位を確立します。

## 規範的ソリューションを決定する

組織のコンテキストにおいてリスクと改善の機会を理解したら、軽減策についてチームと協力してください。このフェーズでは、各チームがそれぞれの分野で見つかった HRI に取り組み、HRI に対処するための規範的なソリューションを決定する必要があります。

このステップでは、追加の調査、議論、概念実証の構築が必要になる場合があります。このフェーズでは、ソリューションの実装の詳細にあまり多くの時間を費やさないことが重要です。問題の HRI が優先事項であると判断された場合は、後で行われることになります。

このステップの目的は、ソリューションの複雑さと必要なリソースを理解し、時間、複雑さ、影響に基づいてタスクに優先順位を付ける際に、それらを考慮に入れることです。

グループで協力して、HRI の可能な解決策のリストを収集します。高レベルを維持し、実装の詳細には立ち入らないようにします。

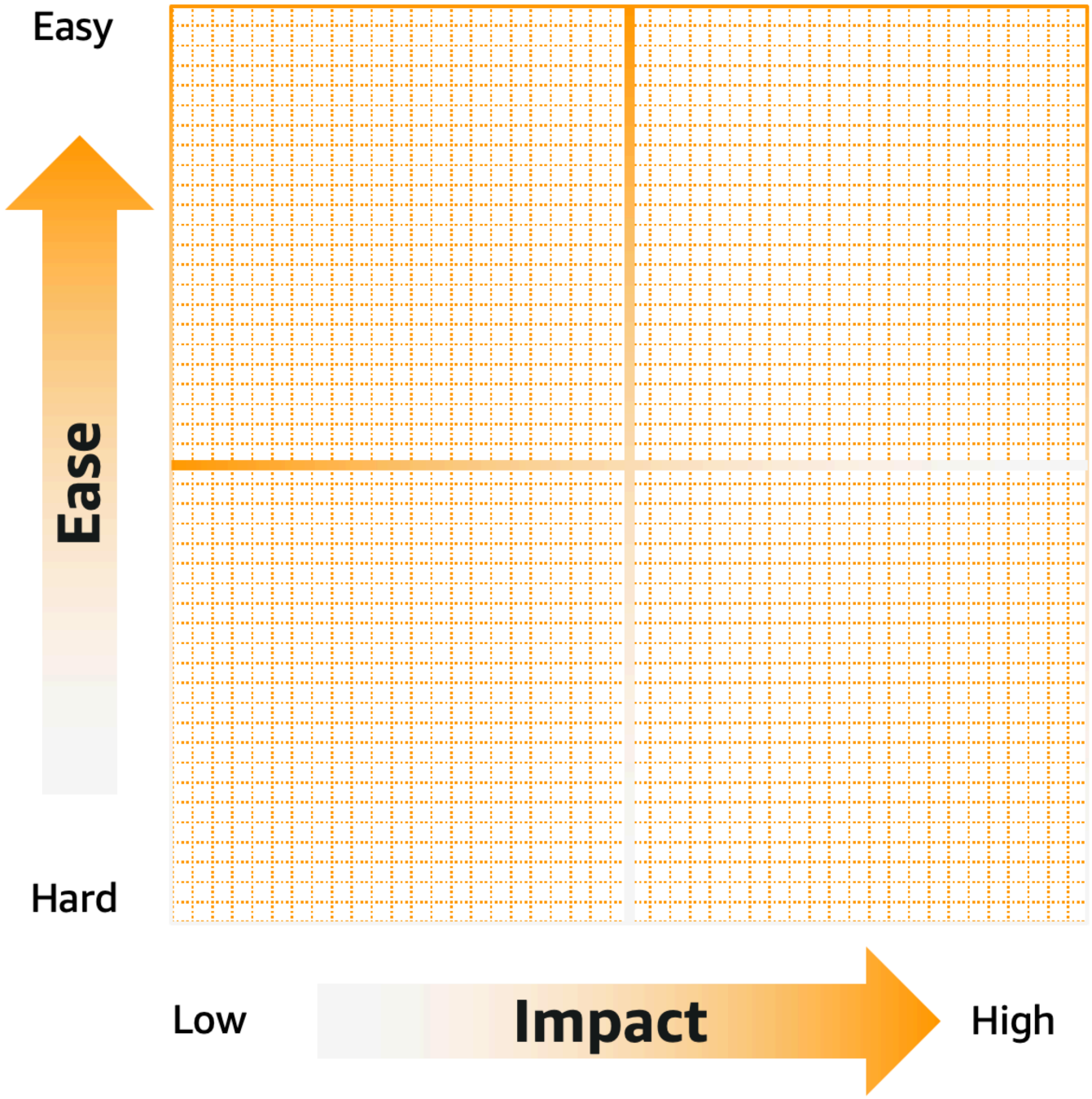
## 改善の優先順位付け

無制限の時間とリソースを持つ組織はありません。特定されたすべての HRI と MRI に一度に対処することは、WAFR を最大限に活用するための正しい方法ではない可能性があります。

まず、ビジネスに最も影響し、実装しやすい選定した数の問題から開始します。ソリューションについて説明します。改善を追跡し、そのアプローチを反復します。

### 実装の優先順位付け

ソリューションの優先度を視覚化するのに役立つアプローチの 1 つは、アイゼンハワースタイルのプロットです。ツールの使用方法はさまざまです。評価する際は、改善の重要性 (ビジネスにもたらす価値) と、改善を実装するための労力 (必要な時間、実装の複雑さ、または人員) の両方を考慮してください。




この分析の出力は、ビジネスに最も影響を与えるが、実装がそれほど複雑ではない一連のリスクを提供します。これらは、最初の反復で実装を開始するのに適した候補です。

## ソリューションの特性

特定されたリスクに対するソリューションを選択するときは、次の点を考慮してください。

- SMART 目標: 具体的、測定可能、達成可能、関連性のある、期限付きの (SMART) 目標について考えます。
- 所有者: ソリューションごとに、所有者を特定します。
- 複雑よりもシンプル: 複雑なソリューションは機能しますが、改善を実装するのが難しくなり、作成に時間がかかる場合があります。複雑なソリューションが交渉不可能な要件でない限り、複雑さよりもシンプルさを選択します。
- 双方向のドアの決定を行う: ソリューションは拡張可能で、時間の経過とともに改善および進化するように設計されている必要があります。可能であれば、アーキテクチャの開発に合わせて適応できない静的ソリューションを避けてください。
- ターゲットパターンベースのソリューション: 体系化、再利用、再共有できるソリューションを検討してください。車輪の再発明はしないでください。例については、AWS アーキテクチャセンターにアクセスしてください。
- チームとして継続的に作業する: グループとして HRI のソリューションのリストを作成します。アイゼンハワーマトリックスで優先順位を付けます。

## 改善の実装と追跡

実装が成功すると、HRI と MRI が減少し、ワークロードのアーキテクチャの健全性が向上します。

修復の実装は、特定の時点でのワークロードの状態を記録する WA ツールのマイルストーンを使用して、繰り返し行う必要があります。レビューセッションを実施するたびに、または改善項目を完了するたびに、マイルストーンを保存して進行状況を測定します。

### アジャイルでの WAFR

WAFR 優先順位付け演習からの出力を使用して、開発チームのスプリントとバックログのチケットに優先順位を付けることができます。開発者は、実装の影響を理解し、アーキテクチャの健全性の向上に貢献できる必要があります。WAFR の改善と追跡は、アジャイルのレトロスペクティブに統合できます。

レトロスペクティブとは、イテレーションまたはスプリントの最後に行われる会議です。レトロスペクティブでは、チームは反復中に何が起こったかを検討し、今後の改善のためのアクションを特定します。ディスカッションに WAFR レビューを含め、メンバーがアーキテクチャの健全性を強化できるよう支援する理想的なメカニズムです。

### タイムライン

これらのステップのタイムラインは、組織ごとに異なり、固有の課題があるため、組織によって異なります。ただし、AWS の多くのお客様に対して WAFR が成功したことを踏まえ、このフェーズに 90～180 日かけることをお勧めします。

HRI と MRI のリストに時間がかかる場合は、優先順位を付け直して短いリストを作成することで、改善のためのプロセスの実践を開始できます。次に、残りの項目で繰り返します。

## WAFR の後のタイムライン

WAFR の 1 日後:

1. 改善計画を含む要約 E メールを作成し、以下をまとめます。
   - レビューの参加者
   - 主な検出結果
   - 次のステップのタイムライン
2. 改善計画をアタッチする
3. チームに計画を指示する

WAFR から 2～3 日後:

1. HRI 優先順位付けミーティングを作成し、HRI の優先順位を決定します。
   - 労力別
   - 影響別
   - ワークロードを担当するチーム
2. ビジネスにとって本当に重要な点について協力する

WAFR から 1 週間後:

1. 改善計画を開始する
2. 次の推奨事項を検討します。
   - 期間: 90 日または 180 日
   - 優先度の高い HRI を特定する
   - それぞれの緩和策を策定する

- 複数の HRI を解決するための取り組みを最大限に活用する

ルーチンタスク:

1. 改善計画に関するフォローアップミーティングの頻度を確率する
2. ワークロードを改善するために実行するアクションを確認する
3. 次の推奨事項を検討します。
   - 参加者の期待値を設定する
   - WA 質問リンクを送信する
   - フォローアップレビューを実施する

# ワークロード

ワークロードは、リソースと、ビジネス価値をもたらすコード (顧客向けアプリケーションやバックエンドプロセスなど) の集まりです。

ワークロードは、1 つの AWS アカウント内のリソースのサブセットで構成されている場合もあれば、複数の AWS アカウントにまたがる複数のリソースの集合になっている場合もあります。中小企業では、ほんの数ワークロードになる一方、大企業では、数千ワークロードにもなることがあります。

左側のナビゲーションからアクセスできる [Workloads (ワークロード)] ページには、すべてのワークロードに関する情報と、共有されたワークロードが表示されます。

ワークロードごとに以下の情報が表示されます。

名前

ワークロードの名前。

所有者

ワークロードを所有する AWS アカウント ID。

回答された質問

回答された質問の数。

[High risks (高リスク)]

特定された高リスクの問題 (HRI) の数。

[Medium risks (中リスク)]

特定された中リスクの問題 (MRI) の数。

[Improvement status (改善ステータス)]

ワークロードに対して設定した改善ステータス。

- なし
- 未開始
- 進行中
- 完了
- Risk Acknowledged (リスク認識)

最終更新日

ワークロードが最後に更新された日時。

リストからワークロードを選択したら、次の操作を行います。

- ワークロードの詳細をレビューするには、[View details (詳細の表示)] を選択します。
- ワークロードのプロパティを変更するには、[Edit (編集)] を選択します。
- 他の AWS アカウント、ユーザー、AWS Organizations または組織部門 (OU) とのワークロード共有を管理するには、[詳細を表示]、[共有] の順に選択します。
- ワークロードとそのすべてのマイルストーンを削除するには、[Delete (削除)] を選択します。ワークロードの所有者のみがこれを削除できます。

> **Warning**
>
> 削除したワークロードを元に戻すことはできません。ワークロードに関連付けられているすべてのデータが削除されます。

# 高リスクの問題 (HRI) と中リスクの問題 (MRI)

AWS Well-Architected Tool で特定された 高リスクの問題 (HRI) は、ビジネスに重大な悪影響を及ぼす可能性があると AWS が認識した、アーキテクチャおよび運用上の選択肢です。HRI は、組織の運用、資産、個人に影響を及ぼす可能性があります。中リスクの問題 (MRI) もビジネスに悪影響を及ぼす可能性がありますが、その程度は比較的低くなります。これらの問題は、AWS Well-Architected Tool の回答に基づいています。対応するベストプラクティスは、AWS および AWS のお客様に広く適用されます。ここでのベストプラクティスとは、AWS Well-Architected フレームワークとレンズによって定義されるガイダンスです。

> **Note**
>
> これらはあくまでガイドラインであり、お客様はそのベストプラクティスを実践しないことでビジネスにどのような影響があるかを評価し、測定する必要があります。ワークロードにベストプラクティスを適用できない技術的またはビジネス上の具体的な理由がある場合、リスクは示された値よりも低くなる可能性があります。AWS では、お客様がこれらの理由とその理由によるベストプラクティスへの影響を、ワークロードのコメントに記録することをお勧めしています。特定されたすべての HRI と MRI の場合、AWS はお客様に対し、AWS

Well-Architected Tool で定義されているベストプラクティスを実践するようお勧めしています。ベストプラクティスを実装した場合は、AWS Well-Architected Tool でベストプラクティスが実装済みであるとマークして、問題が解決したことを示します。お客様がベストプラクティスを実装しないことを選択した場合、AWS は、実装しない理由と適切なビジネスレベルの承認を記録することをお勧めします。

# AWS Well-Architected Tool でのワークロードの定義

ワークロードを定義するには 2 つの方法があります。AWS WA Tool の [ワークロード] ページでは、テンプレートなしでワークロードを定義できます。または、[レビューテンプレート] ページでは、既存のレビューテンプレートを使用するか、新しいテンプレートを作成して、ワークロードを定義できます。

[ワークロード] ページでワークロードを定義するには

1. 左側のナビゲーションペインで [ワークロード] を選択します。
2. [ワークロードの定義] ドロップダウンを選択します。
3. [ワークロードの定義] を選択します。または、レビューテンプレートを作成していて、そこからワークロードを定義する場合は、[レビューテンプレートから定義] を選択します。
4. the section called “ワークロードの定義” の指示に従って、ワークロードプロパティを指定するか、任意でプロファイルとレンズを適用します。

[レビューテンプレート] ページからワークロードを定義するには

1. 左側のナビゲーションペインで [レビューテンプレート] を選択します。
2. 既存のレビューテンプレートの名前を選択するか、the section called “レビューテンプレートの作成” の指示に従って新しいレビューテンプレートを作成します。
3. [テンプレートからワークロードを定義] を選択します。
4. the section called “テンプレートからのワークロードの定義” の指示に従って、レビューテンプレートからワークロードを作成します。

# AWS Well-Architected Tool でのワークロードの表示

自分が所有しているワークロードと、自分と共有されているワークロードの詳細を表示できます。

ワークロードを表示するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。
3. 以下のいずれかの方法で表示するワークロードを選択します。
   - ワークロードの名前を選択します。
   - ワークロードを選択したら、[詳細の表示] を選択します。

ワークロード詳細ページが表示されます。

> **Note**
>
> 必須フィールド [Review owner (レビューの所有者)] が追加されました。これにより、レビュープロセスの主担当者またはグループを簡単に識別できます。
> このフィールドが追加される前に定義されたワークロードを初めて表示すると、この変更が通知されます。[Edit (編集)] を選択して [Review owner (レビュー所有者)] フィールドを設定します。それ以上のアクションは必要ありません。
> [Acknowledge] (了解) を選択すると、[Review owner] (レビュー所有者) フィールドの設定が延期されます。その 60 日間、フィールドが空白であることを示すバナーが表示されます。バナーを削除するには、ワークロードを編集し、[Review owner (レビュー所有者)] を指定します。
> 指定された日付までにフィールドを設定しない場合、ワークロードへのアクセスが制限されます。ワークロードの表示と削除は続行できますが、[Review owner (レビュー所有者)] フィールドの設定以外は編集できません。ワークロードへの共有アクセスは、アクセスが制限されている間も影響を受けません。

# AWS Well-Architected Tool でのワークロードの編集

自分が所有しているワークロードの詳細を編集できます。

ワークロードを編集するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。

3. 編集するワークロードを選択したら、[Edit (編集)] を選択します。
4. ワークロードに変更を加えます。

   各フィールドの説明については、「AWS WA Tool でのワークロードの定義」を参照してください。

   > **Note**
   >
   > 既存のワークロードを更新する場合、[Trusted Advisor をアクティブ化する] を使用できます。これにより、ワークロード所有者の IAM ロールが自動作成されます。Trusted Advisor が有効化されたワークロードに関連するアカウントの所有者は、IAM でロールを作成する必要があります。詳細については、「the section called “IAM で Trusted Advisor を有効化”」を参照してください。

5. [保存] を選択して、ワークロードに加えた変更を保存します。

   必須フィールドが空白の場合、または指定した値が無効な場合は、ワークロードに対する更新を保存する前に問題を修正する必要があります。

# AWS Well-Architected Tool でのワークロードの共有

自分が所有しているワークロードは、同じ AWS リージョン のその他 AWS アカウント、ユーザー、組織、および組織部門 (OU) と共有できます。

> **Note**
>
> ワークロードを共有できるのは、同じ AWS リージョン内だけです。
> ワークロードを他の AWS アカウント と共有する場合、受信者に `wellarchitected:UpdateShareInvitation` アクセス許可がないと、共有の招待を受け入れることはできません。アクセス許可ポリシーの例については、「the section called “AWS WA Tool へのアクセスの提供”」を参照してください。

他の AWS アカウント やユーザーとワークロードを共有するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。

3. 次のいずれかの方法で、自分が所有しているワークロードを選択します。
   - ワークロードの名前を選択します。
   - ワークロードを選択したら、[詳細を表示] を選択します。
4. [共有] を選択します。次に、[作成]、[ユーザーまたはアカウントへの共有を作成] の順に選択し、ワークロードの招待状を作成します。
5. ワークロードを共有するユーザーの 12 桁の AWS アカウント ID または ARN を入力します。
6. 付与するアクセス許可を選択します。

   読み取り専用

   ワークロードへの読み取り専用アクセスを許可します。

   投稿者

   回答とそのメモへの更新アクセスと、残りのワークロードへの読み取り専用アクセスを許可します。
7. [作成] を選択して、指定した AWS アカウント またはユーザーにワークロードの招待を送信します。

ワークロードの招待が 7 日以内に承諾されない場合、招待は自動的に期限切れになります。

ユーザーとユーザーの AWS アカウント の両方にワークロードの招待がある場合、最高レベルのアクセス許可のワークロードの招待がユーザーに適用されます。

> **Important**
>
> ワークロードを組織または組織部門 (OU) と共有する前に、AWS Organizations アクセスを有効にする必要があります。

ワークロードを組織や OU と共有するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。
3. 次のいずれかの方法で、自分が所有しているワークロードを選択します。
   - ワークロードの名前を選択します。

- ワークロードを選択したら、[詳細を表示] を選択します。

4. [共有] を選択します。次に、[作成] と [Organizations への共有の作成] を選択します。
5. [ワークロード共有を作成] ページで、組織全体に許可を付与するのか、1 つ以上の OU に付与するのかを選択します。
6. 付与するアクセス許可を選択します。

   読み取り専用

   ワークロードへの読み取り専用アクセスを許可します。

   投稿者

   回答とそのメモへの更新アクセスと、残りのワークロードへの読み取り専用アクセスを許可します。
7. [作成] を選択してワークロードを共有します。

ワークロードへのアクセスを共有している人を確認するには、AWS Well-Architected Tool でのワークロードの詳細の表示ページで [Shares] (共有) を選択します。

エンティティによるワークロードの共有を防止するため、`wellarchitected:CreateWorkloadShare` アクションを拒否するポリシーを追加します。

また、自分が所有しているカスタムレンズは、同じ AWS リージョン 内の他の AWS アカウント、ユーザー組織 OU と共有できます。詳細については、「AWS WA Tool でのカスタムレンズの共有」を参照してください。

## AWS Well-Architected Tool ワークロードを共有するときの考慮事項

ワークロードは、最大 20 の異なる AWS アカウント およびユーザーと共有できます。ワークロードを共有できるのは、ワークロードと同じ AWS リージョンにあるアカウントとユーザーのみです。

2019 年 3 月 20 日以降に開設されたリージョンでワークロードを共有するには、自分と共有先の AWS アカウントの両方が AWS マネジメントコンソール でそのリージョンを有効にする必要があります。詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

ワークロードは、AWS アカウント、アカウントの個々のユーザー、またはその両方と共有できます。ワークロードを AWS アカウント と共有すると、そのアカウントのすべてのユーザーにワークロードへのアクセスが付与されます。アカウントの特定のユーザーだけがアクセスを必要とする場合

は、最小特権付与のベストプラクティスに従い、それらのユーザーと個別にワークロードを共有します。

AWS アカウント と、アカウントのユーザーの両方にワークロードの招待がある場合、最高レベルのアクセス許可が付与されているワークロード招待が、ワークロードへのユーザーのアクセス許可を判断します。ユーザーのワークロードの招待を削除した場合、ユーザーのアクセスは AWS アカウントのワークロードの招待によって決まります。ワークロードへのユーザーのアクセス権を削除するには、両方のワークロードの招待を削除します。

ワークロードを組織または 1 つ以上の組織部門 (OU) と共有する前に、AWS Organizations アクセスを有効にする必要があります。

1 つの組織と 1 つ以上の OU の両方とワークロードを共有する場合、最高レベルのアクセス許可を持つワークロード招待によって、そのワークロードに対するアカウントのアクセス許可が決まります。

AWS Organizations 共有を有効にするには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool コンソールを開きます。
2. 左側のナビゲーションペインで [設定] を選択します。
3. [AWS Organizations のサポートを有効化] を選択します。
4. [設定を保存] を選択します。

## AWS Well-Architected Tool での共有アクセスの削除

ワークロードの招待は削除できます。ワークロードの招待を削除すると、ワークロードへの共有アクセスが削除されます。

ワークロードへの共有アクセスを削除するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。
3. 以下のいずれかの方法でワークロードを選択します。
   - ワークロードの名前を選択します。
   - ワークロードを選択したら、[詳細を表示] を選択します。
4. [共有] を選択します。

5. 削除するワークロードの招待を選択し、[削除] を選択します。
6. [Delete] を選択して確定します。

ユーザーとユーザーの AWS アカウント にワークロードの招待がある場合、ワークロードに対するユーザーのアクセス許可を削除するには、両方のワークロードの招待を削除する必要があります。

## AWS Well-Architected Tool での共有アクセスの変更

保留中または承諾されたワークロードの招待を変更できます。

ワークロードへの共有アクセスを変更するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。
3. 次のいずれかの方法で、自分が所有しているワークロードを選択します。
   - ワークロードの名前を選択します。
   - ワークロードを選択したら、[詳細を表示] を選択します。
4. [共有] を選択します。
5. 変更するワークロードの招待を選択し、[編集] を選択します。
6. AWS アカウント またはユーザーに付与する新しいアクセス許可を選択します。

   読み取り専用

   ワークロードへの読み取り専用アクセスを許可します。

   投稿者

   回答とそのメモへの更新アクセスと、残りのワークロードへの読み取り専用アクセスを許可します。
7. [保存] を選択します。

変更したワークロードの招待が 7 日以内に承諾されない場合は、自動的に期限切れになります。

## AWS Well-Architected Tool でのワークロードの招待の承諾と拒否

ワークロードの招待は、別の AWS アカウントが所有するワークロードを共有するためのリクエストです。ワークロードの招待を承諾すると、ワークロードが [ワークロード] ページと [ダッシュボード]

ページに追加されます。ワークロードの招待を拒否すると、その招待はワークロードの招待リストから削除されます。

ワークロードの招待を承諾するまでに、7 日の猶予があります。7 日以内に招待を承諾しない場合は、自動的に期限切れになります。

> **Note**
>
> ワークロードは、同じ AWS リージョン内でのみ共有できます。

ワークロードの招待を承諾または拒否するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで、[Workload invitations (ワークロードの招待)] を選択します。
3. 承諾または拒否するワークロードの招待を選択します。
   - ワークロードの招待を承諾するには、[承諾] を選択します。

     ワークロードが [ワークロード] ページと [ダッシュボード] ページに追加されます。
   - ワークロードの招待を拒否するには、[拒否] を選択します。

     ワークロードの招待がリストから削除されます。

ワークロードの招待が承諾された後に共有アクセスを拒否するには、ワークロードのAWS Well-Architected Tool でのワークロードの詳細の表示ページで [Reject share] (共有を拒否) を選択します。

# AWS Well-Architected Tool でのワークロードの削除

不要になったワークロードは削除できます。ワークロードを削除すると、マイルストーンやワークロード共有の招待も含め、ワークロードに関連付けられているすべてのデータが削除されます。ワークロードを削除できるのは、ワークロードの所有者だけです。

> **Warning**
>
> 削除したワークロードを元に戻すことはできません。ワークロードに関連付けられているすべてのデータが完全に削除されます。

ワークロードを削除するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。
3. 削除するワークロードを選択したら、[Delete (削除)] を選択します。
4. [Delete (削除)] ウィンドウで、[Delete (削除)] を選択してワークロードとそのマイルストーンの削除を確認します。

エンティティによるワークロードの削除を防止するため、`wellarchitected:DeleteWorkload` アクションを拒否するポリシーを追加します。

# AWS Well-Architected Tool でのワークロードレポートの生成

レンズのワークロードレポートを生成できます。レポートには、ワークロードの質問への回答、コメント、特定された現在の中および高リスクの数が含まれています。質問で 1 つ以上のリスクが特定された場合、その質問のための改善計画により、それらのリスクを軽減するためのアクションが一覧表示されます。

ワークロードにプロファイルが関連付けられている場合は、プロファイルの概要情報と優先順位付けされたリスクがワークロードレポートに表示されます。

レポートを使用すると、AWS Well-Architected Tool にアクセスできない他のユーザーとワークロードに関する詳細を共有できます。

ワークロードレポートを生成するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。
3. 目的のワークロードを選択したら、[詳細を表示] を選択します。

4. レポートを生成するレンズを選択したら、[レポート生成] を選択します。

   レポートが生成され、そのダウンロードや表示が可能になります。

# AWS Well-Architected Tool でのワークロードの詳細の表示

ワークロード詳細ページには、マイルストーン、改善計画、ワークロード共有など、ワークロードに関する情報が表示されます。ページ上部のタブを使用して、さまざまな詳細セクションに移動します。

ワークロードを削除するには、[Delete workload (ワークロードの削除)] を選択します。ワークロードを削除できるのは、ワークロードの所有者だけです。

共有ワークロードへのアクセスを削除するには、[Reject share (共有の拒否)] を選択します。

トピック

- AWS Well-Architected Tool の [概要] タブ
- AWS Well-Architected Tool の [マイルストーン] タブ
- AWS Well-Architected Tool の [プロパティ] タブ
- AWS Well-Architected Tool の [共有] タブ

## AWS Well-Architected Tool の [概要] タブ

初めてワークロードを表示したときには、まず [Overview (概要)] タブが表示されます。このタブには、ワークロードの全体的な状態、続いて各レンズの状態が表示されます。

すべての質問を完了していない場合は、ワークロードのドキュメント化を開始または続行するよう促すバナーが表示されます。

[Workload overview (ワークロードの概要)] セクションには、ワークロードの現在の全体的な状態と、[Workload notes (ワークロードコメント)] に入力したコメントが表示されます。状態またはコメントを更新するには、[Edit (編集)] を選択します。

ワークロードの現在の状態を記録するには、[Save milestone (マイルストーンの保存)] を選択します。マイルストーンは不変であり、保存後に変更することはできません。

ワークロードの状態の文書化を続けるには、[Start reviewing (レビューの開始)] を選択し、目的のレンズを選択します。

## AWS Well-Architected Tool の [マイルストーン] タブ

ワークロードのマイルストーンを表示するには、[Milestones (マイルストーン)] タブを選択します。

マイルストーンを選択したら、[レポートの生成] を選択して、マイルストーンに関連付けられたワークロードレポートを作成します。レポートには、ワークロードの質問への回答、コメント、マイルストーンが保存された時点での、ワークロードの中および高リスクの数が含まれています。

以下のいずれかの方法で、特定のマイルストーンの時点におけるワークロードの状態に関する詳細を表示できます。

- マイルストーンの名前を選択します。
- マイルストーンを選択したら、[View milestone (マイルストーンの表示)] を選択します。

## AWS Well-Architected Tool の [プロパティ] タブ

ワークロードのプロパティを表示するには、[Properties (プロパティ)] タブを選択します。これらのプロパティの初期値は、ワークロードの定義時に指定された値です。[Edit (編集)] を選択して、変更を加えることができます。変更できるのは、ワークロードの所有者だけです。

プロパティの説明については、「AWS WA Tool でのワークロードの定義」を参照してください。

## AWS Well-Architected Tool の [共有] タブ

ワークロードの招待を表示または変更するには、[共有] タブを選択します。このタブは、ワークロードの所有者に対してのみ表示されます。

ワークロードへの共有アクセスを持つ各 AWS アカウント とユーザーごとに、次の情報が表示されます。

Principal

ワークロードへの共有アクセスを持つ AWS アカウント ID またはユーザー ARN。

ステータス

ワークロード招待のステータス。

- 保留中

  招待は承諾または拒否待ちです。ワークロードの招待が 7 日以内に承諾されない場合は、自動的に期限切れになります。

- 承諾

  招待は承諾されました。
- 拒否

  招待は拒否されました。
- 失効済み

  招待は 7 日以内に承諾または拒否されませんでした。

アクセス許可

AWS アカウント またはユーザーに付与されるアクセス許可。

- 読み取り専用

  プリンシパルは、ワークロードに対する読み取り専用アクセス権を持ちます。
- コントロビューター

  プリンシパルは回答とそのメモを更新でき、残りのワークロードへの読み取り専用アクセス権を持ちます。

許可の詳細

アクセス許可の詳細説明。

同じ AWS リージョン 内の別の AWS アカウント またはユーザーとワークロードを共有するには、[作成] を選択します。ワークロードは、最大 20 の異なる AWS アカウント およびユーザーと共有できます。

ワークロードの招待を削除するには、招待を選択して [削除] を選択します。

ワークロードの招待を変更するには、招待を選択し、[編集] を選択します。

# AWS WA Tool でのレンズの使用

AWS Well-Architected Tool では、レンズを使用することで、一貫した方法でアーキテクチャをベストプラクティスに照らして評価し、改善すべき分野を特定できます。ワークロードが定義されると、AWS Well-Architected フレームワークレンズが自動適用されます。

ワークロードには、1 つまたは複数のレンズを適用できます。各レンズには、それぞれ独自の質問、ベストプラクティス、コメント、改善計画があります。

ワークロードに適用できるレンズには、[レンズカタログ] と [カスタムレンズ] の 2 種類があります。

- レンズカタログ: AWS によって作成され、管理されている公式レンズ。レンズカタログはすべてのユーザーが利用でき、追加でインストールしなくても使用できます。
- カスタムレンズ: AWS の公式コンテンツではない、ユーザー定義のレンズ。独自の柱、質問、ベストプラクティス、改善計画を使用して、カスタムレンズを作成したり、他の AWS アカウントとカスタムレンズを共有したりできます。

一度に 5 つのレンズをワークロードに追加でき、1 つのワークロードには最大 20 のレンズを適用できます。

ワークロードからレンズを削除すると、レンズに関連付けられたデータが保持されます。ワークロードにレンズを追加し直した場合、データが復元されます。

## AWS WA Tool でのワークロードへのレンズの追加

ワークロードにレンズを追加すると、アーキテクチャの長所と弱点をよりよく理解し、改善点を特定し、ワークロードがベストプラクティスに従っていることを確認するために役立ちます。

ワークロードにレンズを追加するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。
3. 目的のワークロードを選択したら、[詳細を表示] を選択します。
4. 追加するレンズを選択し、[保存] を選択します。

レンズは、[カスタムレンズ]、[レンズカタログ]、またはその両方から選択できます。

ワークロードには最大 20 個のレンズを追加できます。

AWS レンズカタログの詳細については、「AWS Well-Architected レンズ」を参照してください。すべてのレンズのホワイトペーパーがレンズカタログにレンズとして提供されているわけではありません。

> **免責事項**
>
> 他の AWS ユーザーまたはアカウントが作成したカスタムレンズにアクセスする、またはそれらを適用する (あるいはその両方) ことで、他のユーザーが作成、共有したカスタムレンズが、AWS カスタマーアグリーメントに定義されているサードパーティーコンテンツであることを認めるものとします。

## AWS WA Tool でのワークロードからのレンズの削除

ワークロードとの関連性がなくなったレンズは削除できます。

ワークロードからレンズを削除するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [ワークロード] を選択します。
3. 目的のワークロードを選択したら、[詳細を表示] を選択します。
4. 削除するレンズを選択解除し、[保存] を選択します。

   AWS Well-Architected フレームワークレンズをワークロードから削除することはできません。

レンズに関連するデータは保持されます。レンズをワークロードに戻すと、データが復元されます。

## AWS WA Tool でのワークロードのレンズに関する詳細の表示

レンズに関する詳細は、AWS Well-Architected Tool コンソールで確認できます。レンズの詳細を表示するには、レンズを選択します。

## [概要] タブ

[Overview (概要)] タブには、回答された質問の数など、レンズに関する一般的な情報が表示されます。このタブから続けて、ワークロードの確認、レポートの生成、レンズメモの編集を行うことができます。

## [Improvement Plan] (改善計画) タブ

[Improvement Plan (改善計画)] タブには、ワークロードを改善するために推奨されるアクションのリストが表示されます。リスクと柱に基づいて推奨事項をフィルタ処理できます。

## [Shares] (共有) タブ

カスタムレンズの場合、[Shares] (共有) タブには、そのレンズが共有されている IAM プリンシパルのリストが表示されます。

# AWS WA Tool のワークロード用のカスタムレンズ

独自の柱、質問、ベストプラクティス、改善計画を使用して、カスタムレンズを作成できます。AWS が提供するレンズと同じように、カスタムレンズをワークロードに適用します。また、自分が作成したカスタムレンズを他の AWS アカウントと共有したり、他の人が所有するカスタムレンズを自分と共有したりできます。

カスタムレンズの質問は、特定のテクノロジーに特化したり、組織内のガバナンスニーズに対応したり、Well-Architected フレームワークや AWS レンズで提供されるガイダンスを拡張したりできるようにカスタマイズできます。既存のレンズと同様に、マイルストーンを作成して経時的な進行状況を追跡し、レポートを生成して定期的なステータスを提供できます。

トピック

- AWS WA Tool でのカスタムレンズの表示
- AWS WA Tool でのワークロード用カスタムレンズの作成
- AWS WA Tool でのワークロード用カスタムレンズのプレビュー
- AWS WA Tool でのカスタムレンズの初回公開
- AWS WA Tool でのカスタムレンズの更新の公開
- AWS WA Tool でのカスタムレンズの共有
- AWS WA Tool でのカスタムレンズへのタグの追加

- AWS WA Tool でのカスタムレンズの削除
- AWS WA Tool のレンズ形式の仕様

## AWS WA Tool でのカスタムレンズの表示

自分が所有しているカスタムレンズと、自分と共有されているカスタムレンズの詳細を表示できます。

レンズを表示するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [カスタムレンズ] を選択します。

   > **Note**
   >
   > カスタムレンズを作成していない場合や、カスタムレンズを共有していない場合、[カスタムレンズ] セクションには何も表示されません。

3. 表示するカスタムレンズを選択します。
   - [Owned by me] (自分が所有) – 自分が作成したカスタムレンズを表示します。
   - [Shared with me] (自分と共有) – 自分と共有されているカスタムレンズを表示します。
4. 以下のいずれかの方法で、表示するカスタムレンズを選択します。
   - レンズの名前を選択します。
   - レンズを選択したら、[View details] (詳細の表示) を選択します。

[AWS WA Tool でのワークロードのレンズに関する詳細の表示] ページが表示されます。

[Custom lenses] (カスタムレンズ) ページには以下のフィールドがあります。

名前

レンズの名前。

所有者

カスタムレンズを所有する AWS アカウント ID。

ステータス

[PUBLISHED] (公開済み) というステータスは、カスタムレンズが公開済みで、ワークロードに適用したり他の AWS アカウントと共有したりできることを意味します。

[DRAFT] (下書き) のステータスは、カスタムレンズが作成されたものの、まだ公開されていないことを意味します。カスタムレンズは、ワークロードに適用または共有する前に、公開する必要があります。

バージョン

カスタムレンズのバージョン名。

最終更新日

カスタムレンズが最後に更新された日時。

## AWS WA Tool でのワークロード用カスタムレンズの作成

カスタムレンズを作成するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左のナビゲーションペインで [Custom lenses] (カスタムレンズ) を選択します。
3. [Create custom lens] (カスタムレンズの作成) を選択します。
4. JSON テンプレートファイルをダウンロードするには、[Download file] (ファイルのダウンロード) を選択します。
5. 任意のテキストエディタで JSON テンプレートファイルを開き、カスタムレンズのデータを追加します。このデータには、柱、質問、ベストプラクティス、改善計画リンクが含まれます。

   詳細については、「AWS WA Tool のレンズ形式の仕様」を参照してください。カスタムレンズのサイズは 500 KB を超えることはできません。
6. [ファイルを選択] を選択し、JSON ファイルを選択します。
7. (オプション) [タグ] セクションで、ワークロードレンズに関連付けるタグを追加します。
8. [送信とプレビュー] を選択してカスタムレンズをプレビューするか[送信] を選択して、プレビューせずにカスタムレンズを送信します。

[送信とプレビュー] を選択してカスタムレンズをプレビューして送信する場合は、[次へ] を選択すると、レンズのプレビューに移動できます。[プレビューの終了] を選択すると、[カスタムレンズ] に戻れます。

検証に失敗した場合は、JSON ファイルを編集して、カスタムレンズを再度作成してみてください。

JSON ファイルが AWS WA Tool によって検証されると、カスタムレンズが [Custom lenses] (カスタムレンズ) に表示されます。

カスタムレンズが作成されると、[DRAFT](下書き) ステータスになります。レンズをワークロードに適用したり他の AWS アカウントと共有したりするには、レンズを公開する必要があります。

AWS アカウントでは 最大 15 個のカスタムレンズを作成できます。

> **免責事項**
>
> カスタムレンズにエンドユーザーまたはその他の個人を特定できる情報 (PII) を含めたり、カスタムレンズを介してこれらを収集したりしないでください。自分のカスタムレンズ、または自分のアカウントで使用している共有されたカスタムレンズに PII が含まれる、またはこれらを介して PII が収集される場合、お客様は、含まれる PII が適用法に従って処理されること、適切なプライバシー通知を行うこと、および当該データを処理するために必要な同意を得ることに責任を負います。

## AWS WA Tool でのワークロード用カスタムレンズのプレビュー

カスタムレンズをプレビューするには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [カスタムレンズ] を選択します。
3. プレビューできるのは [下書き] ステータスのレンズだけです。目的の [下書き] カスタムレンズ、[プレビューエクスペリエンス] の順に選択します。
4. [次へ] を選択して、レンズのプレビューを確認します。
5. (オプション) プレビューの各質問内のベストプラクティスを選択し、[回答に基づいて更新する] を選択してリスクロジックをテストすることで、[改善計画] を確認できます。変更が必要な場合は、公開前に JSON テンプレート内の [リスクルール] を更新します。

6. [プレビューを終了] を選択してカスタムレンズに戻ります。

> **Note**
>
> カスタムレンズの作成時に、[送信とプレビュー] を選択しても、カスタムレンズをプレビューできます。

## AWS WA Tool でのカスタムレンズの初回公開

カスタムレンズを公開するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左のナビゲーションペインで [Custom lenses] (カスタムレンズ) を選択します。
3. 目的のカスタムレンズを選択し、[Publish lens] (レンズを公開) を選択します。
4. [Version name] (バージョン名) ボックスに、バージョン変更のための一意の識別子を入力します。この値は最大 32 文字で、英数字とピリオド (「.」) のみを使用できます。
5. [Publish custom lens] (カスタムレンズを公開) を選択します。

   カスタムレンズが発行されると、[発行済み] ステータスになります。

これで、カスタムレンズをワークロードに適用したり、他の AWS アカウント またはユーザーを共有できるようになります。

## AWS WA Tool でのカスタムレンズの更新の公開

既存のカスタムレンズの更新を公開するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左のナビゲーションペインで [Custom lenses] (カスタムレンズ) を選択します。
3. 目的のカスタムレンズを選択し、[Edit] (編集) を選択します。
4. 更新された JSON ファイルの準備ができていない場合は、[Download file] (ファイルをダウンロード) を選択して、現在のカスタムレンズのコピーをダウンロードします。ダウンロードした JSON ファイルを任意のテキストエディタで編集し、必要な変更を加えます。

5. [ファイルを選択] を選択して更新された JSON ファイルし、[送信とプレビュー] を選択してカスタムレンズをプレビューするか、[送信] を選択して、プレビューせずにカスタムレンズを送信します。

   カスタムレンズのサイズは 500 KB を超えることはできません。

   JSON ファイルが AWS WA Tool によって検証されると、カスタムレンズが [Custom lenses] (カスタムレンズ) に [DRAFT] (下書き) ステータスで表示されます。
6. 再度カスタムレンズを選択し、[Publish lens] (レンズを公開) を選択します。
7. [Review changes before publish] (公開前に変更内容を確認) を選択すると、カスタムレンズに加えた変更が正しいかどうかを確認できます。これには、次の確認が含まれます。

   - カスタムレンズの名前
   - 柱の名前
   - 新規作成、更新、削除された質問

   [次へ] を選択します。
8. バージョン変更の種類を指定します。

   メジャーバージョン

   レンズに大きな変更が加えられたことを示します。カスタムレンズの意味に影響を与える変更に使用します。

   レンズが適用されたワークロードには、カスタムレンズの新しいバージョンが利用可能であることが通知されます。

   バージョンの大きな変更は、レンズを使用しているワークロードには自動的に適用されません。

   マイナーバージョン

   レンズに小さな変更が加えられたことを示します。テキストの変更や URL リンクの更新など、小さな変更に使用します。

   バージョンの小さな変更は、カスタムレンズを使用しているワークロードに自動的に適用されます。

   [次へ] を選択します。

9. [Version name] (バージョン名) ボックスに、バージョン変更のための一意の識別子を入力します。この値は最大 32 文字で、英数字とピリオド (「.」) のみを使用できます。
10. [Publish custom lens] (カスタムレンズを公開) を選択します。

    カスタムレンズが発行されると、[発行済み] ステータスになります。

これで、更新されたカスタムレンズをワークロードに適用したり、他の AWS アカウント やユーザーと共有したりできます。

更新がバージョンの大きな変更である場合、旧バージョンのレンズが適用されているワークロードには、新しいバージョンが利用可能であることが通知され、アップグレードのオプションが提示されます。

バージョンの小さな更新は、通知なしで自動的に適用されます。

カスタムレンズのバージョンは、最大 100 バージョンまで作成できます。

## AWS WA Tool でのカスタムレンズの共有

カスタムレンズは、他の AWS アカウント、ユーザー、AWS Organizations および組織部門 (OU) と共有できます。

カスタムレンズを他の AWS アカウント およびユーザーと共有するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左のナビゲーションペインで [Custom lenses] (カスタムレンズ) を選択します。
3. 共有するカスタムレンズを選択したら、[View details] (詳細の表示) を選択します。
4. [AWS WA Tool でのワークロードのレンズに関する詳細の表示] ページで、[共有] を選択します。次に、[作成]、[ユーザーまたはアカウントへの共有を作成] の順に選択し、レンズ共有の招待を作成します。
5. カスタムレンズを共有するユーザーの 12 桁の AWS アカウント ID または ARN を入力します。
6. [作成] を選択して、指定した AWS アカウント または ユーザーにレンズ共有の招待を送信します。

カスタムレンズは、最大 300 の AWS アカウント またはユーザーと共有できます。

レンズ共有の招待が 7 日以内に承諾されない場合、招待は自動的に期限切れになります。

> **Important**
>
> カスタムレンズを組織または組織部門 (OU) と共有する前に、AWS Organizations アクセスを有効化する必要があります。

カスタムレンズを組織または OU と共有するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左側のナビゲーションペインで [カスタムレンズ] を選択します。
3. 共有するカスタムレンズを選択します。
4. [AWS WA Tool でのワークロードのレンズに関する詳細の表示] ページで、[共有] を選択します。次に、[作成] と [Organizations への共有の作成] を選択します。
5. [カスタムレンズ共有を作成] ページで、アクセス許可を組織全体に付与するのか、1 つ以上の OU に付与するのかを選択します。
6. [作成] を選択してカスタムレンズを共有します。

カスタムレンズへの共有アクセスを持つ人を確認するには、AWS WA Tool でのワークロードのレンズに関する詳細の表示ページで [Shares] (共有) を選択します。

> **免責事項**
>
> 自分のカスタムレンズを他の AWS アカウント と共有することで、AWS が自分のカスタムレンズを他のアカウントで利用できるようにすることを認めるものとします。自分の AWS アカウントからカスタムレンズを削除したり、AWS アカウントを終了したりした場合でも、これらの他のアカウントでは共有されたカスタムレンズに引き続きアクセスし、使用できます。

## AWS WA Tool でのカスタムレンズへのタグの追加

カスタムレンズにタグを追加するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。

2. 左側のナビゲーションペインで [カスタムレンズ] を選択します。
3. 更新するカスタムレンズを選択します。
4. [タグ] セクションで、[タグを管理] を選択します。
5. [新しいタグの追加] を選択し、追加する各タグに[キー] および [値] を入力します。
6. [保存] を選択します。

タグを削除するには、削除するタグの横にある[削除] を選択します。

## AWS WA Tool でのカスタムレンズの削除

カスタムレンズを削除するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. 左のナビゲーションペインで [Custom lenses] (カスタムレンズ) を選択します。
3. 削除するカスタムレンズを選択したら、[Delete] (削除) を選択します。
4. [削除] を選択します。

   レンズが適用された既存のワークロードには、カスタムレンズが削除されたことが通知されますが、引き続き使用できます。新しいワークロードにカスタムレンズを適用できなくなりました。

> **免責事項**
>
> 自分のカスタムレンズを他の AWS アカウント と共有することで、AWS が自分のカスタムレンズを他のアカウントで利用できるようにすることを認めるものとします。自分の AWS アカウントからカスタムレンズを削除したり、AWS アカウントを終了したりした場合でも、これらの他のアカウントでは共有されたカスタムレンズに引き続きアクセスし、使用できます。

## AWS WA Tool のレンズ形式の仕様

レンズは特定の JSON 形式を使用して定義されます。カスタムレンズの作成を開始する際に、テンプレートの JSON ファイルをダウンロードするオプションがあります。このファイルで柱、質問、ベストプラクティス、および改善計画の基本構造を定義するため、これをカスタムレンズの基礎として使用できます。

## [Lens] (レンズ) セクション

このセクションでは、カスタムレンズ自体の属性を定義します。これには、名前と説明が含まれます。

- schemaVersion: 使用するカスタムレンズスキーマのバージョン。テンプレートによって設定されます。変更しないでください。
- name: レンズの名前。名前は最大 128 文字です。
- description: レンズの説明文。このテキストは、ワークロードの作成時に追加するレンズを選択するとき、または後で既存のワークロードに適用するレンズを選択するときに表示されます。説明は最大 2,048 文字です。

```
    "schemaVersion": "2021-11-01",
    "name": "Company Policy ABC",
    "description": "This lens provides a set of specific questions to assess compliance
with company policy ABC-2021 as revised on 2021/09/01.",
```

## [Pillars] (柱) セクション

このセクションでは、カスタムレンズに関連する柱を定義します。質問を、AWS Well-Architected フレームワークの柱にマッピングしたり、独自の柱を定義したりできます (あるいはその両方)。

カスタムレンズには最大 10 の柱を定義できます。

- id: 柱の ID。ID は 3 ~ 128 文字で、英数字とアンダースコア (「_」) のみ使用できます。柱に使用される ID は一意である必要があります。

  質問をフレームワークの柱にマッピングするときは、次の ID を使用します。

  - operationalExcellence
  - security
  - reliability
  - performance
  - costOptimization
  - sustainability
- name: 柱の名前。名前は最大 128 文字です。

```
    "pillars": [
       {
           "id": "company_Privacy",
           "name": "Privacy Excellence",
           .
           .
           .
       },
       {
           "id": "company_Security",
           "name": "Security",
           .
           .
           .
       }
    ]
```

## [Questions] (質問) セクション

このセクションでは、柱に関連する質問を定義します。

カスタムレンズの柱には最大 20 の質問を定義できます。

- id: 質問の ID。ID は 3 ~ 128 文字で、英数字とアンダースコア (「_」) のみ使用できます。質問に使用される ID は一意である必要があります。
- title: 質問のタイトル。タイトルは最大 128 文字です。
- description: 質問について詳しく説明します。説明は最大 2,048 文字です。
- helpfulResource displayText: オプション。質問に関する有用な情報を提供するテキスト。テキストは最大 2,048 文字です。helpfulResource url を指定する場合は必ず指定します。
- helpfulResource url: オプション。質問をより詳細に説明する URL リソース。URL は、http:// または https:// で始まる必要があります。

> **Note**
>
> カスタムレンズワークロードを Jira に同期する場合、質問には、質問の「id」と「title」の両方が表示されます。
> Jira チケットで使用される形式は [ QuestionID ] QuestionTitle です。

```
"questions": [
    {
        "id": "privacy01",
        "title": "How do you ensure HR conversations are private?",
        "description": "Career and benefits discussions should occur on secure channels
 only and be audited regularly for compliance.",
        "helpfulResource": {
            "displayText": "This is helpful text for the first question",
            "url": "https://example.com/poptquest01_help.html"
        },
        .
        .
        .
    },
    {
        "id": "privacy02",
        "title": "Is your team following the company privacy policy?",
        "description": "Our company requires customers to opt-in to data use and does
 not disclose customer data to third parties either individually or in aggregate.",
        "helpfulResource": {
            "displayText": "This is helpful text for the second question",
            "url": "https://example.com/poptquest02_help.html"
        },
        .
        .
        .
    }
]
```

## [Choice] (選択肢) セクション

このセクションでは、質問に関連付けられている選択肢を定義します。

カスタムレンズの質問には最大 15 の選択肢を定義できます。

- id: 選択肢の ID。ID は 3 ~ 128 文字で、英数字とアンダースコア (「_」) のみ使用できます。質問の選択肢ごとに固有の ID を指定する必要があります。サフィックスが _no の選択肢を追加すると、質問では None of these の選択肢として扱われます。
- title: 選択肢のタイトル。タイトルは最大 128 文字です。
- helpfulResource displayText: オプション。選択肢に関する有用な情報を提供するテキスト。テキストは最大 2,048 文字です。helpfulResource url を指定する場合は必ず含めます。

- helpfulResource url: オプション。選択肢をより詳細に説明する URL リソース。URL は、http:// または https:// で始まる必要があります。
- improvementPlan displayText: 選択肢の改善方法を説明するテキスト。テキストは最大 2,048 文字です。None of these の選択肢を除き、各選択肢には improvementPlan が必要です。
- improvementPlan url: オプション。改善に役立つ URL リソース。URL は、http:// または https:// で始まる必要があります。
- additionalResources type: オプション。追加リソースのタイプ。この値は HELPFUL_RESOURCE または IMPROVEMENT_PLAN となります。
- additionalResources content: オプション。追加リソースに対して、displayText および url の値を指定します。選択肢には、役立つ追加リソースを最大 5 つと、追加の改善計画項目を 5 つまで指定できます。
  - displayText: オプション。役に立つリソースまたは改善計画を説明するテキスト。テキストは最大 2,048 文字です。url を指定する場合は必ず含めます。
  - url: オプション。役に立つリソースや改善計画の URL リソース。URL は、http:// または https:// で始まる必要があります。

> **Note**
>
> カスタムレンズワークロードを Jira に同期する場合、選択には、質問と選択の「id」および選択の「title」が表示されます。
> 使用される形式は [ QuestionID | ChoiceID ] ChoiceTitle です。

```
    "choices": [
         {
             "id": "choice_1",
             "title": "Option 1",
             "helpfulResource": {
                 "displayText": "This is helpful text for the first choice",
                 "url": "https://example.com/popt01_help.html"
             },
             "improvementPlan": {
                 "displayText": "This is text that will be shown for improvement of
this choice.",
                 "url": "https://example.com/popt01_iplan.html"
             }
```

```
        },
        {
            "id": "choice_2",
            "title": "Option 2",
            "helpfulResource": {
                "displayText": "This is helpful text for the second choice",
                "url": "https://example.com/hr_manual_CORP_1.pdf"
            },
            "improvementPlan": {
                "displayText": "This is text that will be shown for improvement of
this choice.",
                "url": "https://example.com/popt02_iplan_01.html"
            },
            "additionalResources":[
               {
                 "type": "HELPFUL_RESOURCE",
                 "content": [
                   {
                     "displayText": "This is the second set of helpful text for this
choice.",
                     "url": "https://example.com/hr_manual_country.html"
                   },
                   {
                     "displayText": "This is the third set of helpful text for this
choice.",
                     "url": "https://example.com/hr_manual_city.html"
                   }
                 ]
               },
               {
                 "type": "IMPROVEMENT_PLAN",
                 "content": [
                   {
                     "displayText": "This is additional text that will be shown for
improvement of this choice.",
                     "url": "https://example.com/popt02_iplan_02.html"
                   },
                   {
                     "displayText": "This is the third piece of improvement plan
text.",
                     "url": "https://example.com/popt02_iplan_03.html"
                   }
                   {
```

```
                    "displayText": "This is the fourth piece of improvement plan
text.",
                    "url": "https://example.com/popt02_iplan_04.html"
                  }
                ]
              }
            ]
        },
        {
             "id": "option_no",
             "title": "None of these",
             "helpfulResource": {
               "displayText": "Choose this if your workload does not follow these best
practices.",
               "url": "https://example.com/popt02_iplan_none.html"
             }

           }
```

## [Risk Rules] (リスクルール) セクション

このセクションでは、選択した選択肢がリスクレベルを決定する方法を定義します。

質問ごとに最大 3 つのリスクルールを定義できます (リスクレベルごとに 1 つ)。

- condition: 質問のリスクレベルに対応する選択肢のブール式、または default。

  各質問には、default リスクルールが必要です。
- risk: 条件に関連するリスクを示します。有効な値は、HIGH_RISK、MEDIUM_RISK、NO_RISK です。

リスクルールの順序は重要です。true に評価された最初の condition によって、その質問のリスクが設定されます。リスクルールを実装する一般的なパターンは、まずリスクが最も低い (そして一般的に最も詳細な) ルールから実装し、最後にリスクが最も高い (および最も限定的でない) ルールを実装することです。

例:

```
"riskRules": [
      {
        "condition": "choice_1 && choice_2 && choice_3",
```

```
        "risk": "NO_RISK"
      },
      {
        "condition": "((choice_1 || choice_2) && choice_3) || (!choice_1 &&
choice_3)",
        "risk": "MEDIUM_RISK"
      },
      {
        "condition": "default",
        "risk": "HIGH_RISK"
      }
]
```

質問に 3 つの選択肢がある場合 (choice_1、choice_2、choice_3) の場合、これらのリスクルールは次のように動作します。

- 3 つの選択肢がすべて選択されている場合、リスクなし。
- choice_1 または choice_2 のいずれかが選択され、かつ choice_3 が選択された場合、中リスク。
- choice_1 が選択されず、choice_3 が選択された場合も中リスクとなります。
- 上記の条件のいずれにも当てはまらない場合、高リスク。

# AWS WA Tool でのレンズのアップグレード

AWS Well-Architected フレームワークレンズおよびその他の AWS 提供のレンズは、新しいサービスの導入、クラウドベースのシステムに関する既存のベストプラクティスの改善、新しいベストプラクティスの追加に伴い、更新されます。新しいバージョンのレンズが使用可能になると、AWS WA Tool は最新のベストプラクティスを反映するようにアップグレードされます。定義された新しいワークロードでは、新しいバージョンのレンズが使用されます。

レンズは、ワークロードに適用したカスタムレンズまたは、レビューテンプレートに新しいメジャーなバージョンが公開された場合にも、アップグレードされます。

レンズのアップグレードは、以下のいずれかの組み合わせで構成されます。

- 新しい質問やベストプラクティスの追加
- 推奨されなくなった古い質問やプラクティスの削除
- 既存の質問またはベストプラクティスの更新

- 柱の追加または削除

既存の質問に対する回答は保持されます。

> **Note**
>
> レンズアップグレードを元に戻すことはできません。ワークロードを最新のレンズバージョンにアップグレードした後に、以前のバージョンのレンズに戻ることはできません。

## AWS WA Tool でのアップグレードするレンズの特定

[通知] ページを表示すると、最新のレンズバージョンを使用していないワークロードを確認できます。

[通知] ページには、ワークロードごとに以下の情報が表示されます。

リソース

ワークロードまたはレビューテンプレートの名前。

リソースタイプ

リソースのタイプ。これはワークロードまたはレビューテンプレートのいずれかとなります。

関連付けられたリソース

レンズの名前。

[通知タイプ]

アップグレード通知のタイプ。

- [Not current (最新でない)] - ワークロードには、最新でなくなったバージョンのレンズが使用されています。改良されたガイダンスを表示するには、最新バージョンのレンズにアップグレードしてください。
- [Deprecated] (廃止) - ワークロードには、ベストプラクティスを反映しなくなったバージョンのレンズが使用されています。最新バージョンのレンズにアップグレードします。
- [Deleted] (削除) - ワークロードは、所有者によって削除されたレンズを使用しています。

[Version in use] (使用中のバージョン)

ワークロードに現在使用されているレンズのバージョン。

[Current available version (現在使用可能なバージョン)]

アップグレード可能なレンズのバージョン。レンズが削除されている場合は [None] (なし) と表示されます。

ワークロードに関連付けられているレンズをアップグレードするには、ワークロード名を選択しから、[Upgrade lens version (レンズのバージョンのアップグレード)] を選択します。

## AWS WA Tool でのレンズのアップグレード

レンズはワークロードとレビューテンプレートに合わせてアップグレードできます。

> **Note**
>
> レンズアップグレードを元に戻すことはできません。ワークロードまたはレビューテンプレートを最新のレンズバージョンにアップグレードした後は、レンズの前のバージョンに戻すことはできません。

ワークロード用のレンズのアップグレード

1. [通知] ページで、アップグレードするワークロードを選択し、[レンズバージョンをアップグレード] を選択します。各柱の変更内容に関する情報が表示されます。

   > **Note**
   >
   > ワークロードの [概要] タブから [利用可能なアップグレードを表示] を選択することもできます。

2. ワークロードのレンズをアップグレードする前に、今後の参照用に既存のワークロードの状態を保存するためのマイルストーンが作成されます。マイルストーンの一意の名前を [マイルストーン名] フィールドに入力します。
3. [これらの変更を理解し、受け入れます] の横にある [確認] ボックスを選択し、[保存] を選択します。

レンズをアップグレードすると、[マイルストーン] タブで以前のバージョンのレンズを表示できます。

レビューテンプレート用のレンズのアップグレード

1. レビューテンプレート用にレンズをアップグレードするには、以下を選択します。
2. [通知] ページで、アップグレードするレビューテンプレートを選択し、[レンズバージョンをアップグレード] を選択します。各柱の変更内容に関する情報が表示されます。

   > **Note**
   >
   > レビューテンプレートの [概要] タブから [利用可能なアップグレードを表示] を選択することもできます。

3. [これらの変更を理解し、受け入れます] の横にある [確認] ボックスを選択し、[アップグレードしてテンプレートの回答を編集] を選択してレビューテンプレートのベストプラクティスの質問への回答を調整するか、[アップグレード] を選択してテンプレートの回答を調整せずにレンズをアップグレードします。

# AWS WA Tool のレンズカタログ

[レンズカタログ] は、AWS Well-Architected Tool 向けに作成された AWS の公式レンズのコレクションで、最新のテクノロジーと業界別に的を絞ったベストプラクティスを提供します。これらのレンズはすべてのユーザーが利用でき、追加でインストールしなくても使用できます。

以下の表は、現在レンズカタログで入手可能なすべてのAWS 公式レンズをまとめたものです。

| レンズ名 | 説明 |
| --- | --- |
| AWS Well-Architected フレームワーク | デフォルトですべてのワークロードに適用されます。信頼性、セキュリティ、効率、コスト効果が高く、持続可能なシステムを設計し、クラウド内で運用するためのアーキテクチャのベストプラクティスのコレクションです。 |
| コネクテッドモビリティ | テクノロジーを輸送システムに統合し、全体的なモビリティエクスペリエンスを強化するためのベストプラクティスです。 |
| コンテナビルド | コンテナの設計と構築プロセスに関するベストプラクティスを提供します。 |

| レンズ名 | 説明 |
| --- | --- |
| データ分析 | 実際の導入事例から AWS が収集したインサイトが含まれており、Well-Architected 分析ワークロードの主要な設計要素と、改善のための推奨事項を学ぶのに役立ちます。 |
| DevOps | 最新テクノロジーと DevOps のベストプラクティスを使用して、十分なビジネス価値を提供できる高速でセキュリティ重視の文化を育成する、あらゆる規模の組織に適用可能な構造化されたアプローチを表します。 |
| 金融サービス業界 | AWS で金融サービス業界のワークロードを設計するためのベストプラクティスです。 |
| 生成 AI | AWS で生成 AI ワークロードを設計するためのベストプラクティス。 |
| 政府 | AWS で政府サービスを設計および提供するためのベストプラクティスです。 |
| ヘルスケア業界 | AWS クラウドでのヘルスケアワークロードの設計、デプロイ、管理方法に関するベストプラクティスとガイダンスです。 |
| IoT | AWS でモノのインターネット (IoT) ワークロードを管理するためのベストプラクティスです。 |
| 合併と買収 | 合併や買収を実施するときのワークロードの統合とクラウドへの移行に関するベストプラクティスです。 |
| 機械学習 | AWS で機械学習リソースとワークロードを管理するためのベストプラクティスです。 |
| 移行 | AWS クラウドへの移行方法に関するベストプラクティスです。 |

| レンズ名 | 説明 |
| --- | --- |
| SaaS | AWS クラウド での Software as a Service (SaaS) ワークロードの設計、デプロイ、構築に焦点を当てています。 |
| SAP | AWS クラウドでの SAP ワークロードの設計原則とベストプラクティスです。 |
| サーバーレスアプリケーション | AWS 上にサーバーレスワークロードを構築するためのベストプラクティス。RESTful マイクロサービス、モバイルアプリケーションバックエンド、ストリーム処理、ウェブアプリケーションなどのシナリオについて取り上げます。 |

# AWS WA Tool のレビューテンプレート

Well-Architected フレームワークとカスタムレンズのベストプラクティスに関する質問への回答があらかじめ入力された AWS WA Tool でレビューテンプレートを作成できます。Well-Architected レビューテンプレートがあれば、Well-Architected レビューを実施する際に、複数のワークロードに共通するベストプラクティスについて同じ回答を手動で入力する必要がなくなり、チームやワークロード全体でベストプラクティスの一貫性と標準化を促進できます。

レビューテンプレートを作成すると、ベストプラクティスに関する一般的な質問に回答したり、メモを作成したりできます。メモは、別の IAM ユーザーやアカウント、あるいは同じ AWS リージョン内の組織や組織部門と共有できます。レビューテンプレートからワークロードを定義できます。これにより、一般的なベストプラクティスを拡張し、ワークロード全体の冗長性を減らすことができます。

## AWS WA Tool でのレビューテンプレートの作成

レビューテンプレートを作成するには

1. 左側のナビゲーションペインで [レビューテンプレート] を選択します。
2. [テンプレートを作成] をクリックします。
3. [テンプレートの詳細を指定] ページで、レビューテンプレートの [名前] と [説明] を入力します。
4. (オプション) [テンプレートノート] セクションと [タグ] セクションに、レビューテンプレートに関連付けるテンプレートノートまたはタグを追加します。追加したメモはレビューテンプレートを使用するすべてのワークロードに適用されますが、タグはレビューテンプレートに固有のものです。

   タグの詳細については、「AWS WA Tool リソースのタグ付け」を参照してください。
5. [次へ] を選択します。
6. [レンズを適用] ページで、レビューテンプレートに適用するレンズを選択します。適用できるレンズの数は最大 20 です。

   レンズは、[カスタムレンズ]、[レンズカタログ]、またはその両方から選択できます。

> **Note**
>
> 共有されているレンズはレビューテンプレートには適用できません。

7. [テンプレートを作成] をクリックします。

作成したレビューテンプレートに関する質問への回答を開始するには

1. テンプレートの [概要] タブの [質問への回答を開始] 情報アラートにある、[質問に答える] ドロップダウンでレンズを選択します。

> **Note**
>
> [レンズ] セクションに移動してレンズを選択し、[質問に答える] を選択することもできます。

2. レビューテンプレートに適用した各レンズについて、該当する質問に答え、完了したら [保存して終了] を選択します。

レビューテンプレートを作成したら、そのテンプレートから新しいワークロードを定義できます。

レビューテンプレートの [概要] タブには、[テンプレートの詳細] セクションで回答された質問の合計数と、[レンズ] セクションの各レンズについて回答された質問の数が反映されます。

# AWS WA Tool でのレビューテンプレートの編集

レビューテンプレートを編集するには

1. 左側のナビゲーションペインで [レビューテンプレート] を選択します。
2. 編集するレビューテンプレートの名前を選択します。
3. レビューテンプレートの [名前]、[説明]、または [テンプレートノート] を更新するには、[概要] タブの [テンプレートの詳細] セクションで [編集] を選択します。
   a. [名前]、[説明]、または [テンプレートノート] を変更します。
   b. [テンプレートを保存] を選択し、変更内容を反映してレビューテンプレートを更新します。
4. レビューテンプレートに適用するレンズを更新するには、[概要] タブの [レンズ] セクションで、[適用したレンズを編集] を選択します。

a. 追加または削除するレンズのチェックボックスをオンまたはオフにします。

レンズは、[カスタムレンズ]、[レンズカタログ]、またはその両方から選択あるいは選択解除できます。

b. [テンプレートを保存] を選択し、変更を保存します。

5. レンズに関するベストプラクティスの質問への回答を更新するには、[概要] タブの [レンズ] セクションでレンズの名前を選択します。

a. [レンズの概要] セクションで、[質問に答える] を選択します。

> **Note**
>
> オプションで、左側のナビゲーションペインにある [レビューテンプレート] ドロップダウンでレンズの名前を選択すると、[レンズの概要] セクションに移動できます。

b. 変更するベストプラクティスの回答の横にあるチェックボックスをオンまたはオフにします。

c. [保存] を選択して、変更を保存して適用します。

# AWS WA Tool でのレビューテンプレートの共有

レビューテンプレートは、ユーザーやアカウントと共有することも、組織全体または組織部門と共有することもできます。

レビューテンプレートを共有するには

1. 左側のナビゲーションペインで [レビューテンプレート] を選択します。
2. 共有するレビューテンプレートの名前を選択します。
3. [共有] タブを選択します。
4. ユーザーまたはアカウントと共有するには、[作成] を選択し、[IAM ユーザーまたはアカウントと共有] を選択します。[招待を送信] ボックスで、ユーザー ID またはアカウント ID を指定し、[作成] を選択します。
5. 組織または組織部門と共有するには、[作成] を選択し、[Organizations と共有] を選択します。組織全体で共有するには、[組織全体に許可を付与] を選択します。組織部門と共有するには、[個々の組織部門に許可を付与] を選択し、ボックスで組織部門を指定して [作成] を選択します。

> **Important**
>
> プロファイルを組織または組織部門 (OU) と共有する前に、AWS Organizations アクセスを有効にする必要があります。

# AWS WA Tool でのテンプレートからのワークロードの定義

作成したレビューテンプレートまたは共有されているレビューテンプレートからワークロードを定義できます。削除されたレビューテンプレートから新しいワークロードを定義することはできません。レビューテンプレートに古いバージョンのレンズが含まれている場合は、レビューテンプレートをアップグレードしてから新しいワークロードを定義する必要があります。レビューテンプレートのアップグレード方法の詳細については、「the section called “レンズのアップグレード”」を参照してください。

> **Note**
>
> レビューテンプレートからワークロードを定義するには、ワークロードを作成するための IAM アクセス許可 `wellarchitected:CreateWorkload` および `wellarchitected:GetReviewTemplate`、`wellarchitected:GetReviewTemplateAnswer`、`w` のレビューテンプレート権限が有効になっている必要があります。IAM アクセス許可の詳細については、「AWS Identity and Access Management ユーザーガイド」を参照してください。

レビューテンプレートからワークロードを定義するには

1. 左側のナビゲーションペインで [レビューテンプレート] を選択します。
2. ワークロードを定義するレビューテンプレートの名前を選択します。
3. [テンプレートからワークロードを定義] を選択します。

   > **Note**
   >
   > [ワークロード] ページの [ワークロードの定義] ドロップダウンから [レビューテンプレートから定義] を選択することもできます。

4. [レビューテンプレートを選択] で、レビューテンプレートカードを選択し、[次へ] を選択します。

5. [プロパティを指定] で、ワークロードプロパティの必須フィールドに入力して [次へ] を選択します。詳細については、「the section called “ワークロードの定義”」を参照してください。
6. (オプション) [プロファイルの適用] では、既存のプロファイルを選択するか、プロファイル名を検索するか、[プロファイルを作成] を選択してプロファイルを作成し、プロファイルをワークロードに関連付けます。[次へ] をクリックします。

   Well-Architected プロファイルとレビューテンプレートは組み合わせて使用できます。レビューテンプレートに事前入力された質問はワークロードで引き続き回答され、質問にはプロファイルに基づいて優先順位が付けられます。
7. (オプション) [レンズを適用] 手順では、レビューテンプレートにまだ適用されていないレンズを、[カスタムレンズ] または [レンズカタログ] から追加で適用することもできます。
8. [ワークロードの定義] を選択します。

# AWS WA Tool でのレビューテンプレートの削除

レビューテンプレートを削除するには

1. 左側のナビゲーションペインで [レビューテンプレート] を選択します。
2. [レビューテンプレート] セクションで、削除するレビューテンプレートを選択し、[アクション] ドロップダウンで [削除] を選択します。

   > **Note**
   >
   > テンプレートの名前を選択し、レビューテンプレートの [概要] タブから [削除] を選択することもできます。
3. レビューテンプレートの [削除] ダイアログボックスにあるフィールドにレビューテンプレートの名前を入力し、削除を確認します。
4. [削除] をクリックします。

削除されたレビューテンプレートから新しいワークロードを作成することはできません。削除したレビューテンプレートを他の IAM ユーザー、アカウント、または組織と共有した場合、そのレビューテンプレートからワークロードを作成することはできません。

# AWS WA Tool でのプロファイルの使用

プロファイルを作成して、ビジネスコンテキストを提供すると、Well-Architected レビューを実施する際に達成したい目標を特定できます。AWS Well-Architected Tool は、プロファイルから収集した情報を使用して、ワークロードレビュー中にビジネスに関連する質問の優先リストに集中できるようにサポートします。ワークロードにプロファイルを添付すると、改善計画で対処すべき優先リスクを確認するのにも役立ちます。

[プロファイル] ページからプロファイルを作成して新しいワークロードに関連付けることも、既存のワークロードにプロファイルを追加することもできます。

## プロファイルの作成

プロファイルを作成するには

1. 左側のナビゲーションペインで [プロファイル] を選択します。
2. [Create profile] (プロファイルの作成) を選択します。
3. [プロファイルのプロパティ] セクションで、プロファイルの [名前] と [説明] を入力します。
4. ワークロードレビューと改善計画の中でビジネスに対して優先度が高い情報を絞り込むには、[プロファイルに関する質問] セクションで、ビジネスに最も関連性がある回答を選択します。
5. (オプション) [タグ] セクションで、プロファイルに関連付けるタグを追加します。

   タグの詳細については、「AWS WA Tool リソースのタグ付け」を参照してください。
6. [保存] を選択します。プロファイルが正常に作成されると、成功メッセージが表示されます。

プロファイルが作成されると、プロファイルの概要が表示されます。概要には、名前、説明、ARN、作成日と更新日、プロファイルに関する質問への回答など、プロファイルに関連するデータが表示されます。[プロファイルの概要] ページでは、プロフィールを編集、削除、共有できます。

# AWS WA Tool でのプロファイルの編集

プロファイルを編集するには

1. 左側のナビゲーションペインで [プロファイル] を選択するか、ワークロードの [プロファイル] セクションから [プロファイルを表示] を選択します。
2. 更新するプロファイルの名前を選択します。
3. [プロファイル概要] ページで [編集] を選択します。
4. プロファイルの質問に必要な更新を行います。
5. [保存] を選択します。

# AWS WA Tool でのプロファイルの共有

プロファイルは、ユーザー、アカウント、組織全体、組織部門と共有できます。

プロファイルを共有するには

1. 左側のナビゲーションペインで [プロファイル] を選択します。
2. 共有するプロファイルの名前を選択します。
3. [共有] タブを選択します。
4. ユーザーまたはアカウントと共有するには、[作成] を選択し、[IAM ユーザーまたはアカウントへの共有を作成] を選択します。[招待を送信] ボックスで、ユーザー ID またはアカウント ID を指定し、[作成] を選択します。
5. 組織または組織部門と共有するには、[作成]、[Organizations への共有を作成] の順に選択します。組織全体で共有するには、[組織全体に許可を付与] を選択します。組織部門と共有するには、[個々の組織部門に許可を付与] を選択し、ボックスに組織部門を指定して、[作成] を選択します。

> **Important**
>
> プロファイルを組織または組織部門 (OU) と共有する前に、AWS Organizations アクセスを有効にする必要があります。

# AWS WA Tool でのワークロードへのプロファイルの追加

既存のワークロードにプロファイルを追加するか、ワークロードを定義する際に、ワークロードレビュープロセスを加速できます。AWS WA Tool は、プロファイルから収集した情報を使用して、ビジネスに関連するワークロードレビューの質問に優先順位を付けます。

ワークロードを定義する際にプロファイルを追加する方法の詳細については、「the section called “ワークロードの定義”」を参照してください。

既存のワークロードにプロファイルを追加するには

1. 左側のナビゲーションペインで [ワークロード] を選択し、プロファイルに関連付けるワークロードの名前を選択します。

   > **Note**
   >
   > ワークロードに関連付けることができるプロファイルは 1 つだけです。

2. [プロファイル] セクションで [プロファイルの追加] を選択します。
3. 使用可能なプロファイルのリストからワークロードに適用するプロファイルを選択するか、[プロファイルの作成] を選択します。詳細については、「the section called “プロファイルの作成”」を参照してください。
4. [保存] を選択します。

[ワークロードの概要]には、関連するプロファイルの情報に基づいて、優先度の高い質問の回答数と優先度の高いリスクの数が表示されます。[レビューを続ける] を選択すると、ワークロードレビューで優先度の高い質問に回答できます。詳細については、「the section called “ワークロードのドキュメント化”」を参照してください。

[プロファイル] セクションには、ワークロードに関連付けられているプロファイルの名前、説明、ARN、バージョン、最終更新日が表示されます。

# AWS WA Tool でのワークロードからのプロファイルの削除

ワークロードからプロファイルを削除すると、そのワークロードはプロファイルが関連付けられていた以前のバージョンに戻り、ワークロードレビューの質問やリスクは優先されなくなります。

ワークロードからプロファイルを削除するには

1. ワークロードの [プロファイル] セクションで [削除] を選択します。
2. 削除を確認するには、テキスト入力フィールドにプロファイルの名前を入力します。
3. [を削除] を選択します。

プロファイルがワークロードから正常に削除されたことを示す通知が表示されます。ワークロードからプロファイルを削除すると、そのワークロードはプロファイルが関連付けられていた以前のバージョンに戻り、ワークロードレビューの質問やリスクは優先されなくなります。

## AWS WA Tool からのプロファイルの削除

プロファイルを作成すると、AWS WA Tool で利用できるプロファイルのリストからそのプロファイルを削除できます。

[プロファイル] ページからプロファイルを削除しても、関連するワークロードからプロファイルは削除されません。削除前にワークロードと共有、関連付けられていたプロファイルは引き続き使用できますが、削除したプロファイルに新しいワークロードを関連付けることはできません。削除されたプロファイルを使用して the section called “プロファイル通知” がワークロード所有者に送信されます。

> **免責事項**
>
> 自分のプロファイルを他の AWS アカウント と共有することで、AWS が自分のプロファイルを他のアカウントで利用できることを認めたと見なされます。自分の AWS アカウント からプロファイルを削除したり、AWS アカウント を終了したとしても、これらの他のアカウントは、引き続き共有したプロファイルにアクセスして、使用できます。

プロファイルのリストからプロファイルを削除するには

1. 左側のナビゲーションペインで [プロファイル] を選択します。
2. 削除するプロファイルの名前を選択します。
3. [削除] を選択します。
4. 削除を確認するには、テキスト入力フィールドにプロファイルの名前を入力します。
5. [削除] を選択します。

プロファイルを [プロファイル] リストに残し、ワークロードからは削除したい場合は、「the section called “ワークロードからのプロファイルの削除”」を参照してください。

# AWS Well-Architected Tool Connector for Jira

AWS Well-Architected Tool Connector for Jira を使用すると、Jira アカウントを AWS Well-Architected Tool とリンクし、ワークロードから改善項目を Jira プロジェクトに同期して、改善の実装にクローズドループメカニズムを取り入れることができます。

コネクタは自動同期と手動同期の両方を提供します。詳細については、「コネクタの設定」を参照してください。

コネクタは、アカウントレベルとワークロードレベルで設定でき、ワークロードごとにアカウントレベルの設定を上書きするオプションがあります。ワークロードレベルでは、ワークロードを同期から完全に除外することもできます。

改善項目の同期先として、デフォルトの WA Jira プロジェクトを使用するか、既存のプロジェクトキーを指定できます。ワークロードレベルでは、必要に応じて各ワークロードを一意の Jira プロジェクトに同期できます。

> **Note**
>
> コネクタは、Jira のスクラムプロジェクトとカンバンプロジェクトのみをサポートしています。

Jira に同期された改善項目は次のように編成されます。

- プロジェクト: WA (または指定した既存のプロジェクト)
- エピック: ワークロード
- タスク: 質問
- サブタスク: ベストプラクティス
- ラベル: 柱

[設定] ページで Jira アカウントの同期を設定したら、Jira コネクタを設定し、改善項目を Jira アカウントに同期できます。

# コネクタのセットアップ

コネクタをインストールするには

> **Note**
>
> 以下の手順はすべて、AWS アカウントではなく Jira アカウントで実行します。

1. Jira アカウントにログインします。
2. 上部のナビゲーションバーで、[アプリ] を選択し、[その他のアプリを探す] を選択します。
3. [Jira 用のアプリおよび統合の検索] ページで、「AWS Well-Architected」と入力します。次に、[AWS Well-Architected Tool Connector for Jira] を選択します。
4. アプリのページで、[アプリを入手] を選択します。
5. [Jira に追加] ペインで、[今すぐ入手] を選択します。
6. セットアップを完了するには、アプリがインストールされた後、[設定] を選択します。
7. [AWS Well-Architected Tool の設定] ページで、[新しい AWS アカウントを接続] を選択します。
8. [AccessKeyId] と [シークレットキー] を入力します。オプション: [セッショントークン] を入力します。次に、[接続] を選択します。

> **Note**
>
> アカウントに `wellarchitected:ConfigureIntegration` アクセス許可があることを確認します。このアクセス許可は、AWS アカウントを Jira に追加するために必要です。
> 複数の AWS アカウントを AWS WA Tool に接続できます。

> **Note**
>
> セキュリティのベストプラクティスとして、短期の IAM 認証情報を使用することを強くお勧めします。AWS アカウントの [AccessKeyId] と [シークレットキー] を作成する方法の詳細については、「アクセスキーの管理 (コンソール)」を参照してください。短期の認証情報を使用する方法の詳細については、「一時的なセキュリティ認証情報をリクエストする」を参照してください。

9. [リージョン] で、接続する AWS リージョンを選択します。次に、[接続] を選択します。

Jira プロジェクトの設定

カスタムプロジェクトを使用する場合は、プロジェクトの設定に次の課題タイプが含まれていることを確認してください。

- スクラム: エピック、ストーリー、サブタスク
- カンバン: エピック、タスク、サブタスク

課題タイプの管理の詳細については、「アトラシアンサポート | 課題タイプの追加、編集、および削除」を参照してください。

AWS Well-Architected Tool でコネクタのステータスを確認するには

1. AWS アカウントにログインし、AWS Well-Architected Tool に移動します。
2. 左側のナビゲーションペインの [設定] を選択します。
3. [Jira アカウントの同期] セクションの [Jira アプリ接続ステータス] で、ステータスが [設定済み] であることを確認します。

これでコネクタのセットアップが完了し、設定の準備が整いました。Jira の同期設定をアカウントレベルおよびワークロードレベルで構成するには、「コネクタの設定」を参照してください。

# コネクタの設定

AWS Well-Architected Tool Connector for Jira では、Jira の同期をアカウントレベル、ワークロードレベル、またはその両方で設定できます。アカウントレベルの設定に左右されないワークロードレベルの Jira の設定を構成したり、特定のワークロードのアカウントレベルの設定を上書きしてワークロードの同期の動作を指定したりできます。ワークロードを定義するときに Jira の設定を構成することもできます。

コネクタは、自動と手動の 2 つの同期方法を提供します。どちらの同期方法でも、AWS WA Tool で行われた変更は Jira プロジェクトに反映され、Jira で行われた変更は AWS WA Tool に同期されます。

> **Important**
>
> 自動同期を使用すると、AWS WA Tool が Jira での変更に応じてワークロードを変更することに同意したことになります。
> Jira に同期することが望ましくない機密情報がある場合は、その情報をワークロードの [メモ] フィールドに入力しないようにしてください。

- 自動同期: コネクタは、質問が更新されるたびに Jira プロジェクトとワークロードを自動的に更新します。質問の更新には、ベストプラクティスの選択または選択解除や、質問の完了が該当します。
- 手動同期: Jira と AWS WA Tool の間で改善項目を同期するには、ワークロードダッシュボードで [Jira と同期する] を選択する必要があります。同期する特定の柱と質問を選択することもできます。詳細については、「ワークロードの同期」を参照してください。

アカウントレベルでコネクタを設定するには

1. 左側のナビゲーションペインの [設定] を選択します。
2. [Jira アカウントの同期] ペインで、[編集] を選択します。
3. [仮想タイプ] で、次のいずれかを選択します。
   a. 変更が行われたときに自動的にワークロードを同期するには、[自動] を選択します。
   b. ワークロードを同期するタイミングを手動で選択するには、[手動] を選択します。
4. デフォルトでは、コネクタによって WA Jira プロジェクトが作成されます。独自の Jira プロジェクトキーを指定するには、次の手順を実行します。
   a. [デフォルトの Jira プロジェクトキーを上書きする] をオンにします。
   b. [Jira プロジェクトキー] を入力します。

   > **Note**
   >
   > [Jira プロジェクトキー] の指定は、プロジェクトをワークロードレベルで変更しない限り、すべてのワークロードに使用されます。

5. [設定を保存] を選択します。

ワークロードレベルでコネクタを設定するには

1. 左側のナビゲーションペインで [ワークロード] を選択し、設定するワークロードの名前を選択します。
2. [プロパティ] を選択します。
3. [Jira] ペインで、[編集] を選択します。
4. ワークロードの Jira の設定を構成するには、[アカウントレベルの設定を上書き] をオンにします。

   > **Note**
   >
   > ワークロード固有の設定を適用するには、[アカウントレベルの設定を上書き] をオンにする必要があります。

5. [同期オーバーライド] で、次のいずれかを選択します。

   a. ワークロードを Jira の同期から除外するには、[ワークロードを同期しない] を選択します。
   b. ワークロードを同期するタイミングを手動で選択するには、[ワークロードの同期 - 手動] を選択します。
   c. ワークロードの変更を自動的に同期するには、[ワークロードの同期 - 自動] を選択します。

6. (オプション) [Jira プロジェクトキー] に、ワークロードの同期先のプロジェクトキーを入力します。このプロジェクトキーは、アカウントレベルのプロジェクトキーと異なっていてもかまいません。

   プロジェクトキーを指定しない場合は、コネクタによって WA Jira プロジェクトが作成されます。

7. [保存] を選択します。

手動同期の実行方法の詳細については、「ワークロードの同期」を参照してください。

# ワークロードの同期

自動同期では、ワークロードの更新時 (質問を完了したときや新しいベストプラクティスを選択したときなど) に、コネクタによって自動的に改善項目が同期されます。

手動同期と自動同期のどちらでも、Jira で行われた変更 (質問やベストプラクティスの完了など) は AWS Well-Architected Tool に同期されます。

ワークロードを手動で同期するには

1. ワークロードを Jira に同期する準備ができたら、左側のナビゲーションペインで [ワークロード] を選択します。次に、同期するワークロードを選択します。
2. ワークロードの概要で、[Jira と同期する] を選択します。
3. 同期するレンズを選択します。
4. [Jira と同期する質問] で、Jira プロジェクトに同期する質問または柱全体を選択します。
   - 質問を削除する場合は、質問タイトルの横にある [X] アイコンを選択します。
5. [同期] を選択します。

# コネクタのアンインストール

AWS Well-Architected Tool Connector for Jira を完全にアンインストールするには、次のタスクを実行します。

- アカウントレベルの同期設定を上書きするすべてのワークロードで Jira の同期をオフにする
- アカウントレベルで Jira の同期をオフにする
- Jira で AWS アカウントのリンクを解除する
- Jira アカウントからコネクタをアンインストールする

アカウントレベルでコネクタをオフにするには

> **Note**
> 以下の手順は AWS アカウントで実行します。

1. 左側のナビゲーションペインの [設定] を選択します。
2. [Jira アカウントの同期] セクションで、[編集] を選択します。
3. [Jira アカウントの同期を有効にする] オプションをオフにします。
4. [設定を保存] を選択します。

### AWS アカウントのリンクを解除するには

> **Note**
>
> 以下の手順はすべて、AWS アカウントではなく Jira アカウントで実行します。

1. Jira アカウントにログインします。
2. 上部のナビゲーションバーで、[アプリ] を選択し、[アプリの管理] を選択します。
3. [AWS Well-Architected Tool Connector for Jira] の横にあるドロップダウン矢印を選択し、[構成] を選択します。
4. AWS アカウントのリンクを解除するには、AWS Well-Architected Tool の構成ペインで、[アクション] の下にある [X] を選択します。

### コネクタをアンインストールするには

> **Note**
>
> 以下の手順はすべて、AWS アカウントではなく Jira アカウントで実行します。
> コネクタをアンインストールする前に、コネクタの設定で、接続されているすべての AWS アカウントのリンクが解除されていることを確認することをお勧めします。

1. Jira アカウントにログインします。
2. 上部のナビゲーションバーで、[アプリ] を選択し、[アプリの管理] を選択します。
3. [AWS Well-Architected Tool Connector for Jira] の横にあるドロップダウン矢印を選択します。
4. [アンインストール] を選択し、[アプリをアンインストール] を選択します。

# マイルストーン

マイルストーンは、特定の時点におけるワークロードの状態を記録します。

最初に、ワークロードに関連するすべての質問を完了したら、マイルストーンを保存します。改善計画の項目に基づいてワークロードを変更するときに、進捗状況を評価するための追加のマイルストーンを保存できます。

ベストプラクティスは、ワークロードを改善するたびにマイルストーンを保存することです。

## マイルストーンの保存

マイルストーンには、ワークロードの現在のステータスが記録されます。ワークロードの所有者は、いつでもマイルストーンを保存できます。

マイルストーンを保存するには

1. ワークロード詳細ページで、[Save milestone (マイルストーンの保存)] を選択します。
2. [Milestone name (マイルストーン名)] ボックスに、マイルストーンの名前を入力します。

   > **Note**
   >
   > 名前は 3 ~ 100 文字にします。3 文字以上をスペースにしないでください。ワークロードに関連付けられるマイルストーン名は一意にしてください。一意かどうかを確認するときは、スペースと大文字は無視されます。

3. [Save (保存)] を選択してマイルストーンを保存します。

マイルストーンが保存された後は、記録されたワークロードデータを変更することはできません。ワークロードを削除すると、それに関連付けられているマイルストーンも削除されます。

## マイルストーンの表示

以下の方法で、ワークロードのマイルストーンを表示できます。

- ワークロード詳細ページで、[Milestones (マイルストーン)] を選択してから、表示するマイルストーンを選択します。

- [Dashboard (ダッシュボード)] ページの [Milestones (マイルストーン)] セクションでワークロードを選択してから、表示するマイルストーンを選択します。

# マイルストーンレポートの生成

マイルストーンレポートを生成できます。このレポートには、ワークロードの質問、メモ、およびマイルストーンが保存された時点で存在していた中および高リスクに対する応答が含まれます。

レポートを使用すると、AWS Well-Architected Tool にアクセスできない他のユーザーとマイルストーンに関する詳細を共有できます。

マイルストーンレポートを生成するには

1. 以下のいずれかの方法でマイルストーンを選択します。
   - ワークロード詳細ページで、[Milestones (マイルストーン)] を選択してから、マイルストーンを選択します。
   - [Dashboard (ダッシュボード)] ページで、レポートするマイルストーンのワークロードを選択します。[Milestones (マイルストーン)] セクションで、マイルストーンを選択します。
2. [レポートの生成] を選択してレポートを生成します。

   PDF ファイルが生成され、そのダウンロードや表示が可能になります。

# 共有の招待

共有の招待は、別の AWS アカウントが所有するワークロード、カスタムレンズまたはレビューテンプレートを共有するためのリクエストです。ワークロードまたはレンズは、AWS アカウント のすべてのユーザー、個々のユーザー、またはその両方と共有できます。

- ワークロードの招待を承諾すると、そのワークロードが [Workloads] (ワークロード) ページと [Dashboard] (ダッシュボード) ページに追加されます。
- カスタムレンズの招待を承諾すると、そのレンズが [Custom lenses] (カスタムレンズ) ページに追加されます。
- プロフィールの招待を承諾すると、[プロファイル] ページにプロファイルが追加されます。
- レビューテンプレートの招待を承諾すると、[レビューテンプレート] ページにテンプレートが追加されます。

招待を拒否すると、一覧から削除されます。

> **Note**
>
> ワークロード、カスタムレンズ、プロファイルおよびレビューテンプレートは、同じ AWS リージョン 内でのみ共有できます。

ワークロードまたはカスタムレンズの所有者は、共有アクセス権を持つユーザーを管理します。

左側のナビゲーションからアクセスできる [Share invitations] (共有の招待) ページには、ワークロードとカスタムレンズの保留中の招待に関する情報が表示されます。

ワークロードの招待ごとに以下の情報が表示されます。

名前

共有するワークロード、カスタムレンズ、またはレビューテンプレートの名前。

リソースタイプ

招待のタイプ (ワークロード、カスタムレンズ、プロファイル、レビューテンプレートのいずれか)。

[所有者]

ワークロードを所有する AWS アカウント ID。

アクセス許可

ワークロードに対してユーザーに付与されているアクセス許可。

- 読み取り専用

  ワークロード、カスタムレンズ、プロファイルまたはレビューテンプレートへの読み取り専用アクセスを提供します。

- 投稿者

  回答とそのメモへの更新アクセスと、残りのワークロードへの読み取り専用アクセスを許可します。このアクセス許可は、ワークロードの場合にのみ使用できます。

アクセス許可の詳細

アクセス許可の詳細説明。

# 共有の招待の承諾

共有の招待を承諾するには

1. 承諾する共有の招待を選択します。
2. [Accept (承諾)] を選択します。

ワークロードの招待の場合は、そのワークロードが [Workloads] (ワークロード) ページと [Dashboard] (ダッシュボード) ページに追加されます。カスタムレンズの招待の場合は、そのカスタムレンズが [Custom lenses] (カスタムレンズ) ページに追加されます。プロファイル招待の場合、[プロファイル] ページにプロファイルが追加されます。レビューテンプレートの招待の場合、[レビューテンプレート] ページにテンプレートが追加されます。

招待を承諾するまで 7 日間の猶予があります。7 日以内に招待を承諾しない場合は、自動的に期限切れになります。

ユーザーと AWS アカウント の両方がワークロード招待を承諾した場合、ユーザーのワークロード招待がユーザーのアクセス許可を判断します。

# 共有の招待の拒否

共有の招待を拒否するには

1. 拒否するワークロードまたはカスタムレンズの招待を選択します。
2. [拒否] を選択します。

招待がリストから削除されます。

# 通知

[通知] ページには、ワークロードのバージョンの違いと、レンズとプロファイルが関連付けられているレビューテンプレートが表示されます。[通知] ページでは、ワークロードのレンズまたはプロファイルの最新バージョンにアップグレードできます。

## レンズ通知

新しいバージョンのレンズが利用可能になると、[ワークロード] ページまたは [レビューテンプレート] ページの上部にバナーが表示され、通知されます。古いレンズを使用する特定のワークロードまたはレビューテンプレートを表示している場合も、新しいバージョンのレンズが利用可能であることを示すバナーが表示されます。

アップグレード可能なワークロードまたはレビューテンプレートのリストに対して、[利用可能なアップグレードを表示] を選択します。

ワークロードまたはレビューテンプレートにレンズをアップグレードする手順については、「the section called “レンズのアップグレード”」を参照してください。

共有レンズの所有者がレンズを削除したときに、削除したレンズに関連するワークロードがある場合は、既存のワークロードではレンズを引き続き使用できますが、新しいワークロードには追加できないという通知が届きます。

## プロファイル通知

プロファイル通知には、次の 2 種類があります。

- プロファイルのアップグレード
- プロファイルの削除

ワークロードに関連付けられているプロファイルが編集されると (詳細については、「the section called “プロファイルの編集”」を参照)、プロファイルの新しいバージョンがあるという通知が [プロファイル通知] に表示されます。

共有プロファイルの所有者がプロファイルを削除したときに、削除したプロファイルに関連するワークロードがある場合は、既存のワークロードではプロファイルを引き続き使用できますが、新しいワークロードには追加できないという通知が届きます。

プロファイルバージョンをアップグレードするには

1. 左側のナビゲーションペインで、[通知] を選択します。
2. [プロファイル通知] タブのリストからワークロードの名前を選択するか、検索バーを使用してワークロード名で検索します。
3. [プロファイルバージョンのアップグレード] を選択します。
4. [承認] セクションで、[これらの変更を理解し、受け入れます] の確認ボックスを選択します。
5. (オプション) マイルストーンを保存する場合は、[マイルストーンを保存] ボックスを選択し、[マイルストーン名] を指定します。
6. [Save] を選択します。

プロファイルがアップグレードされると、最新のバージョン番号と更新日がワークロードの [プロファイル] セクションに表示されます。

詳細については、「プロファイル」を参照してください。

# ダッシュボード

左側のナビゲーションで使用可能な [ダッシュボード] では、ワークロードとそれらに関連付けられている中リスクの問題および高リスクの問題にアクセスできます。自分と共有されているワークロードを含めることもできます。[ダッシュボード] は 4 つのセクションで構成されます。

- 概要 — すべてのワークロードにおけるワークロードの総数、高リスクと中リスクが割り当てられている数、および高リスクと中リスクの問題の合計数が表示されます。
- Well-Architected フレームワークの柱ごとの問題 — すべてのワークロードについて、高リスクと中リスクの問題を柱ごとにグラフィカルに表示します。
- Well-Architected フレームワークのワークロードごとの問題 — 各ワークロードの高リスクと中リスクの問題を柱ごとに表示します。
- Well-Architected フレームワークの改善計画項目ごとの問題 — すべてのワークロードの改善計画項目を表示します。

## [概要]

このセクションには、Well-Architected フレームワークレンズと他のすべてのレンズ内の、ワークロードの総数と、高リスクと中リスクの問題があるワークロードの数が表示されます。所有または AWS アカウント と共有しているすべてのワークロードにおける高リスクと中リスクの問題の合計数が表示されます。

[自分と共有されているワークロードを含める] を選択すると、統計の概要、統合レポート、およびその他のダッシュボードセクションに、自分のワークロードと自分と共有されているワークロードの両方が反映されます。

[レポートの生成] を選択すると、統合レポートが PDF ファイルとして作成されます。

レポート名の形式は、`wellarchitected_consolidatedreport_`*`account-ID`*`.pdf` です。

## Well-Architected フレームワークの柱ごとの問題

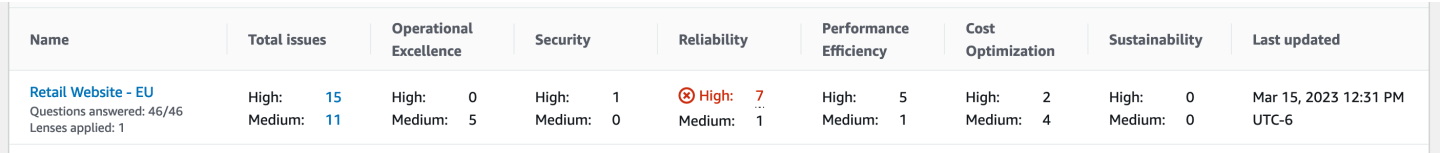
[Well-Architected フレームワークの柱ごとの問題] セクションでは、すべてのワークロードにおける高リスクおよび中リスクの問題の数を柱ごとにグラフで表示しています。

ダッシュボードの残りのセクションを使用すると、ある詳細レベルから次の詳細レベルに移動できます。

> **Note**
>
> このセクションには、Well-Architected フレームワークレンズからの問題のみが含まれています。

# Well-Architected フレームワークのワークロードごとの問題

[Well-Architected フレームワークのワークロードごとの問題] セクションには、各ワークロードの情報が表示されます。



| Name | Total issues | Operational Excellence | Security | Reliability | Performance Efficiency | Cost Optimization | Sustainability | Last updated |
|---|---|---|---|---|---|---|---|---|
| Retail Website - EU<br>Questions answered: 46/46<br>Lenses applied: 1 | High: 15<br>Medium: 11 | High: 0<br>Medium: 5 | High: 1<br>Medium: 0 | High: 7<br>Medium: 1 | High: 5<br>Medium: 1 | High: 2<br>Medium: 4 | High: 0<br>Medium: 0 | Mar 15, 2023 12:31 PM<br>UTC-6 |

ワークロードごとに以下の情報が表示されます。

名前

ワークロードの名前。回答された質問の数と、ワークロードに適用されたレンズの数も表示されます。

ワークロード名を選択すると、[ワークロードの詳細] ページにアクセスして、マイルストーン、改善計画、共有を確認できます。

総問題数

ワークロード用 Well-Architected フレームワークレンズが特定した問題の総数。

高リスクまたは中リスクの問題の数を選択すると、それらの問題に対する推奨改善計画が表示されます。

運用上の優秀性

運用上の優秀性の柱用ワークロードで特定された高リスクの問題 (HRI) および中リスクの問題 (MRI) の数。

セキュリティ

セキュリティの柱で特定された HRI と MRI の数。

信頼性

信頼性の柱で特定された HRI と MRI の数。

パフォーマンス効率

パフォーマンス効率の柱で特定された HRI と MRI の数。

コスト最適化

コスト最適化の柱で特定された HRI と MRI の数。

サステナビリティ

サステナビリティの柱で特定された HRI と MRI の数。

最終更新日

ワークロードが最後に更新された日時。

各ワークロードについて、高リスクの問題 (HRI) の数が最も多い柱が強調表示されます。

> **Note**
>
> このセクションには、Well-Architected フレームワークレンズからの問題のみが含まれています。

# Well-Architected フレームワークの改善計画項目ごとの問題

[Well-Architected フレームワークの改善計画項目ごとの問題] セクションには、すべてのワークロードの改善計画項目が表示されます。項目は柱と重要度に基づいてフィルタリングできます。

各改善計画項目に対して以下の情報が表示されます。

改善項目

改善計画項目の名前。

改善計画項目に関連するベストプラクティスを示す名前を選択します。

柱

改善項目に関連する柱。

Risk

関連する問題が高リスクか中リスクかを示します。

該当するワークロード

この改善計画が適用されるワークロードの数。

改善計画項目を選択すると、該当するワークロードが表示されます。

> **Note**
>
> このセクションには、Well-Architected フレームワークレンズの改善計画項目のみが含まれます。

# AWS Well-Architected Tool でのセキュリティ

AWS でのクラウドセキュリティは最優先事項です。AWS のユーザーは、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを利用できます。

セキュリティは AWS とお客様の間の共有責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ - AWS は、AWS クラウド で AWS のサービスを実行するインフラストラクチャを保護する責任を担います。また、AWS は、ユーザーが安全に使用できるサービスも提供します。AWSコンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。AWS Well-Architected Tool に適用するコンプライアンスプログラムの詳細については、「コンプライアンスプログラムによる対象範囲内の AWS のサービス」「」を参照してください。
- クラウド内のセキュリティ - ユーザーの責任は、使用する AWS のサービスに応じて異なります。また、お客様は、データの機密性、お客様の会社の要件、および適用される法律および規制など、その他の要因についても責任を負います。

このドキュメントは、AWS WA Tool を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために AWS WA Tool を設定する方法を示します。また、AWS WA Tool リソースのモニタリングや保護に役立つ、その他 AWS サービスの使用方法についても説明します。

トピック

# AWS Well-Architected Tool でのデータ保護

AWS 責任共有モデルは、AWS Well-Architected Tool でのデータ保護に適用されます。このモデルで説明されているように、AWS は、AWS クラウド のすべてを実行するグローバルインフラストラクチャを保護するがあります。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「AWS のサービス」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、データプライバシーに関するよくある質問を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された「AWS 責任共有モデルおよび GDPR」のブログ記事を参照してください。

データを保護するため、「AWS アカウント」認証情報を保護し、AWS IAM アイデンティティセンター または AWS Identity and Access Management (IAM) を使用して個々のユーザーをセットアップすることをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
- AWS CloudTrail で API とユーザーアクティビティロギングを設定します。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「AWS CloudTrail ユーザーガイド」の「CloudTrail 証跡の使用」を参照してください。
- AWS のサービス内のすべてのデフォルトセキュリティコントロールに加え、AWS 暗号化ソリューションを使用します。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API を使用して AWS にアクセスする際に FIPS 140-3 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、AWS CLI、または AWS SDK で AWS WA Tool または他の AWS のサービス を使用する場合も同様です。タグ、または名前に使用される自由形式のテキストフィールドに入力されるデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

## 保管中の暗号化

AWS WA Tool によって保存されたすべてのデータは、保管時に暗号化されます。

## 転送中の暗号化

AWS WA Tool との間で送受信されるすべてのデータは、転送中に暗号化されます。

## AWS によるお客様データの使用

AWS Well-Architected チームは、お客様に AWS WA Tool サービスを提供し改善するための集計データを AWS Well-Architected Tool から収集します。個別のお客様データは、お客様のワークロードとアーキテクチャを改善するための取り組みを支援するために AWS アカウントチームと共有されることがあります。AWS Well-Architected チームがアクセスできるのは、ワークロードのプロパティと、各質問に対して選択された選択肢のみです。AWS の外部で、AWS WA Tool からのデータを AWS が共有することはありません。

AWS Well-Architected チームがアクセスできるワークロードプロパティには、次のものが含まれます。

- ワークロード名
- レビュー所有者
- 環境
- リージョン
- アカウント ID
- 業種タイプ

以下には AWS Well-Architected チームからアクセスできません。

- ワークロードの説明
- アーキテクチャの設計
- 入力されたメモ

# AWS Well-Architected Tool のためのアイデンティティおよびアクセス管理

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御するために役立つ AWS のサービス です。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS WA Tool リソースの使用を許可する (権限を持たせる) かを制御します。IAM は、無料で使用できる AWS のサービスです。

トピック



## 対象者

AWS Identity and Access Management (IAM) の使用方法は、ロールによって異なります。

- サービスユーザー - 機能にアクセスできない場合は、管理者にアクセス許可をリクエストします (「AWS Well-Architected Tool ID とアクセスのトラブルシューティング」を参照)。
- サービス管理者 - ユーザーアクセスを決定し、アクセス許可リクエストを送信します (「AWS Well-Architected Tool と IAM の連携方法」を参照)
- IAM 管理者 - アクセスを管理するためのポリシーを作成します (「AWS Well-Architected Tool アイデンティティベースポリシーの例」を参照)

## アイデンティティによる認証

認証とは、アイデンティティ認証情報を使用して AWS にサインインする方法です。ユーザーは、IAM ユーザー の AWS アカウントのルートユーザー として、または IAM ロールを引き受けることによって、認証される 必要があります。

AWS IAM アイデンティティセンター (IAM アイデンティティセンター)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーテッドアイデンティティとしてサインインできます。サインインの詳細については、「AWS サインイン ユーザーガイド」の「AWS アカウントにサインインする方法」を参照してください。

プログラムによるアクセスの場合、AWS はリクエストに暗号で署名するための SDK と CLI を提供します。詳細については、「IAM ユーザーガイド」の「API リクエストに対する AWS 署名バージョン 4」を参照してください。

### AWS アカウント のルートユーザー

AWS アカウントを作成すると、すべての AWS のサービスとリソースに対する完全なアクセス権を持つ AWS アカウント ルートユーザーと呼ばれる 1 つのサインイン ID を使用して開始します。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザー認証情報を必要とするタスクについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

### フェデレーテッドアイデンティティ

ベストプラクティスでは、人間のユーザーが一時的な認証情報を使用して AWS のサービス にアクセスする際、アイデンティティプロバイダーとのフェデレーションを使用することが求められます。

フェデレーテッドアイデンティティは、エンタープライズディレクトリ、ウェブ ID プロバイダー、Directory Service のユーザーであり、ID ソースからの認証情報を使用して AWS のサービスにアクセスするユーザーです。フェデレーテッドアイデンティティは、一時的な認証情報を提供するロールを引き受けます。

アクセスを一元管理する場合は、AWS IAM アイデンティティセンター をお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「IAM アイデンティティセンターとは」を参照してください。

### IAM ユーザーとグループ

IAM ユーザーは、特定の個人やアプリケーションに対する特定のアクセス許可を持つアイデンティティです。長期認証情報を持つ IAM ユーザーの代わりに一時的な認証情報を使用することをお勧めします。詳細は「IAM ユーザーガイド」の「人間のユーザーが一時的な認証情報を使用して AWS にアクセスするには ID プロバイダーとのフェデレーションの使用が必要です」を参照してください。

IAM グループは、IAM ユーザーの集合を指定し、大量のユーザーに対するアクセス許可の管理を容易にします。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

### IAM ロール

IAM ロールは、特定のアクセス許可を持つアイデンティであり、一時的な認証情報を提供します。ユーザーから IAM ロール (コンソール) に切り替える、または AWS CLI や AWS API オペレーションを呼び出すことで、ロールを引き受けることができます。詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーのアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行するアプリケーションに役立ちます。詳細については、IAM ユーザーガイド の IAM でのクロスアカウントリソースアクセス を参照してください。

## ポリシーを使用したアクセス権の管理

AWS でアクセスを制御するには、ポリシーを作成して AWS ID またはリソースにアタッチします。ポリシーは、アイデンティティやリソースとの関連付けに伴うアクセス許可を定義します。AWS は、プリンシパルがリクエストを行うときに、これらのポリシーを評価します。大半のポリシーは JSON ドキュメントとして AWS に保存されます。JSON ポリシードキュメントの詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は、ポリシーを使用して、どのプリンシパルがどのリソースに対して、どのような条件でアクションを実行できるかを定義することで、誰が何にアクセスできるかを指定します。

デフォルトでは、ユーザーやロールにアクセス許可はありません。IAM 管理者は IAM ポリシーを作成してロールに追加し、このロールをユーザーが引き受けられるようにします。IAM ポリシーは、オペレーションの実行方法を問わず、アクセス許可を定義します。

### アイデンティティベースのポリシー

アイデンティティベースのポリシーは、アイデンティティ (ユーザー、グループ、またはロール) にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、アイデンティティがどのリソースに対してどのような条件下でどのようなアクションを実行できるかを制御します。アイデンティティベースポリシーの作成方法については、IAM ユーザーガイド の カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する を参照してください。

アイデンティティベースのポリシーは、インラインポリシー (単一の ID に直接埋め込む) または管理ポリシー (複数の ID にアタッチされたスタンドアロンポリシー) にすることができます。管理ポリシーとインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

## リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。例としては、IAM ロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーで IAM の AWS マネージドポリシーを使用することはできません。

## その他のポリシータイプ

AWS は、より一般的なポリシータイプで付与された最大数のアクセス許可を設定できる、追加のポリシータイプをサポートしています。

- アクセス許可の境界 – アイデンティティベースのポリシーで IAM エンティティに付与することのできるアクセス許可の数の上限を設定します。詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可境界」を参照してください。
- サービスコントロールポリシー (SCP) - AWS Organizations 内の組織または組織単位の最大のアクセス許可を指定します。詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。
- リソースコントロールポリシー (RCP) – は、アカウント内のリソースで利用できる最大数のアクセス許可を定義します。詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。
- セッションポリシー – ロールまたはフェデレーションユーザーの一時セッションを作成する際にパラメータとして渡される高度なポリシーです。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

## 複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成されるアクセス許可を理解するのがさらに難しくなります。複数のポリシータイプが関連するとき、リクエストを許可するかどうかを AWS が決定する方法の詳細については、「IAM ユーザーガイド」の「ポリシーの評価ロジック」を参照してください。

# AWS Well-Architected Tool と IAM の連携方法

IAM を使用して AWS WA Tool へのアクセスを管理する前に、AWS WA Tool で利用できる IAM の機能について学びます。

AWS Well-Architected Tool で使用できる IAM の機能

| IAM 機能 | AWS WA Tool のサポート |
|---|---|
| アイデンティティベースのポリシー | あり |
| リソースベースのポリシー | なし |
| ポリシーアクション | あり |
| ポリシーリソース | はい |
| ポリシー条件キー (サービス固有) | はい |
| ACL | なし |
| ABAC (ポリシー内のタグ) | あり |
| 一時的な認証情報 | あり |
| プリンシパルアクセス権限 | あり |
| サービスロール | いいえ |
| サービスリンクロール | いいえ |

AWS WA Tool およびその他 AWS のサービスがほとんどの IAM 機能と連携する方法の概要を把握するには、「IAM ユーザーガイド」の「IAM と連携する AWS のサービス」を参照してください。

## AWS WA Tool アイデンティティベースのポリシー

ポリシーアクションのサポート: あり

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのようなリソースにどのような条件でアクションを実行できるかということです。

JSON ポリシーの Action 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

## AWS WA Tool 内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーで、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーションユーザー、または AWS のサービス を含めることができます。

クロスアカウントアクセスを有効にするには、全体のアカウント、または別のアカウントの IAM エンティティを、リソースベースのポリシーのプリンシパルとして指定します。詳細については、IAM ユーザーガイドのIAM でのクロスアカウントリソースアクセスを参照してください。

## AWS WA Tool のポリシーアクション

ポリシーアクションのサポート: あり

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのようなリソースにどのような条件でアクションを実行できるかということです。

JSON ポリシーの Action 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。このアクションは、関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

AWS WA Tool のポリシーアクションは、アクションの前に次のプレフィックスを使用します: `wellarchitected:`。たとえば、エンティティがワークロードを定義できるようにするには、管理者は `wellarchitected:CreateWorkload` アクションを許可するポリシーをアタッチする必要があります。同様に、エンティティによるワークロードの削除を防止するため、管理者は `wellarchitected:DeleteWorkload` アクションを拒否するポリシーをアタッチできます。ポリシーステートメントには、Action 要素または NotAction 要素のいずれかを含める必要がありま

す。AWS WA Tool は、このサービスで実行できるタスクを説明する独自の一連のアクションを定義します。

AWS WA Tool アクションのリストを確認するには、「サービス認可リファレンス」の「AWS Well-Architected Tool で定義されるアクション」を参照してください。

## ポリシーリソース

ポリシーリソースのサポート: あり

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

`Resource` JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。リソースレベルの権限をサポートしないアクションの場合は、ワイルドカード (*) を使用してステートメントがすべてのリソースに適用されることを示します。

```
"Resource": "*"
```

AWS WA Tool リソースのタイプとその ARN のリストを確認するには、「サービス認可リファレンス」の「AWS Well-Architected Tool で定義されるリソース」を参照してください。どのアクションで各リソースの ARN を指定できるかについては、「AWS Well-Architected Tool で定義されるアクション」を参照してください。

AWS WA Tool ワークロードリソースには、次の ARN があります。

```
arn:${Partition}:wellarchitected:${Region}:${Account}:workload/${ResourceId}
```

ARN の形式の詳細については、「Amazon リソースネーム (ARN) と AWS サービスの名前空間」を参照してください。

ARN は、ワークロードの [ワークロードのプロパティ] ページにあります。たとえば、特定のワークロードを指定するには、次のようにします。

```
"Resource": "arn:aws:wellarchitected:us-
west-2:123456789012:workload/11112222333344445555666677778888"
```

特定のアカウントに属するすべてのワークロードを指定するには、ワイルドカード (*) を使用します。

```
"Resource": "arn:aws:wellarchitected:us-west-2:123456789012:workload/*"
```

ワークロードの作成とリスト化など、一部の AWS WA Tool アクションは、特定のリソースで実行できません。このような場合はワイルドカード *を使用する必要があります。

```
"Resource": "*"
```

AWS WA Tool リソースのタイプとその ARN のリストを確認するには、サービス認可リファレンスの AWS Well-Architected Tool で定義されるリソースを参照してください。どのアクションで各リソースの ARN を指定できるかについては、「AWS Well-Architected Tool で定義されるアクション」を参照してください。

## AWS WA Tool 向けのポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素は、定義された基準に基づいてステートメントが実行される時期を指定します。イコールや未満などの条件演算子を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。すべての AWS グローバル条件キーを確認するには、IAM ユーザーガイドのAWS グローバル条件コンテキストキーを参照してください。

AWS WA Tool はサービス固有の条件キーを 1 つ提供し (wellarchitected:JiraProjectKey)、いくつかのグローバル条件キーの使用をサポートします。すべての AWS グローバル条件キーを確認するには、「サービス認可リファレンス」の「AWS グローバル条件コンテキストキー」を参照してください。

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素は、定義された基準に基づいてステートメントが実行される時期を指定します。イコールや未満などの条件演算子を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。すべての AWS グローバル条件キーを確認するには、IAM ユーザーガイドのAWS グローバル条件コンテキストキーを参照してください。

## AWS WA Tool の ACL

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするためのアクセス許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

## AWS WA Tool タグに基づく認可

ABAC (ポリシー内のタグ) のサポート: あり

属性ベースのアクセス制御 (ABAC) は、タグと呼ばれる属性に基づいてアクセス許可を定義する認可戦略です。IAM エンティティと AWS リソースにタグを付けることで、プリンシパルのタグがリソースタグと一致するときに操作を許可する ABAC ポリシーを設計できます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用する」を参照してください。

## AWS WA Tool での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一時的な認証情報は、AWSリソースへの短期的なアクセスを提供し、フェデレーションの使用時またはロールの切り替え時に自動的に作成されます。AWS では、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することをお勧めします。詳細については、「IAM ユーザーガイド」の「IAM の一時的な認証情報」および「AWS のサービス と IAM との連携」を参照してください。

## AWS WA Tool のクロスサービスプリンシパル権限

転送アクセスセッション (FAS) のサポート: あり

転送アクセスセッション (FAS) は、AWS のサービス を呼び出すプリンシパルのアクセス許可を AWS のサービス のリクエストと合わせて使用し、ダウンストリームのサービスに対してリクエスト

を行います。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

### AWS WA Tool のサービスロール

サービスロールのサポート: なし

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービス に許可を委任するロールを作成する」を参照してください。

### AWS WA Tool のサービスにリンクされたロール

サービスにリンクされたロールのサポート: なし

サービスにリンクされたロールは、AWS のサービス にリンクされているサービスロールの一種です。サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。サービスにリンクされたロールは、AWS アカウント に表示され、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「IAM と提携する AWS のサービス」を参照してください。表の「サービスリンクロール」列に Yes と記載されたサービスを見つけます。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

## AWS Well-Architected Tool アイデンティティベースポリシーの例

デフォルトでは、ユーザーおよびロールには、AWS WA Tool リソースを作成または変更するアクセス許可はありません。AWS マネジメントコンソール、AWS CLI、または AWS API を使用してタスクを実行することもできません。IAM 管理者は、ユーザーとロールに必要な、指定されたリソースで特定の API オペレーションを実行する権限をユーザーとロールに付与する IAM ポリシーを作成する必要があります。続いて、管理者はそれらのアクセス許可が必要なユーザーまたはグループにそのポリシーをアタッチします。

JSON ポリシードキュメントのこれらの例を使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「JSON タブでのポリシーの作成」を参照してください。

トピック

- ポリシーのベストプラクティス
- AWS WA Tool コンソールを使用する
- ユーザーが自分の許可を表示できるようにする
- ワークロードへのフルアクセスの付与
- ワークロードへの読み取り専用アクセスの付与
- 1 つのワークロードへのアクセス
- AWS Well-Architected Tool Connector for Jira のサービス固有の条件キーの使用

## ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが AWS WA Tool リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、AWS アカウント に料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS マネージドポリシーの使用を開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードへのアクセス許可の付与を開始するには、多くの一般的なユースケースのためにアクセス許可を付与する AWS マネージドポリシーを使用します。これらは AWS アカウントで使用できます。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。詳細については、IAM ユーザーガイド の AWS マネージドポリシー または ジョブ機能の AWS マネージドポリシー を参照してください。
- 最小特権を適用する – IAM ポリシーでアクセス許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイド の IAM でのポリシーとアクセス許可 を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。たとえば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。また、CloudFormation などの特定の AWS のサービス を介して使用する場合、条件を使用してサービスアクションへのアクセスを許可することもできます。詳細については、IAM ユーザーガイド の IAM JSON ポリシー要素:条件 を参照してください。
- IAM アクセスアナライザー を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM アクセスアナライザー は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライ

ザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイド の IAM Access Analyzer でポリシーを検証する を参照してください。

- 多要素認証 (MFA) を要求する – AWS アカウントで IAM ユーザーまたはルートユーザーを要求するシナリオがある場合は、セキュリティを強化するために MFA をオンにします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイド の MFA を使用した安全な API アクセス を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイド の IAM でのセキュリティのベストプラクティス を参照してください。

## AWS WA Tool コンソールを使用する

AWS Well-Architected Tool コンソールにアクセスするには、一連の最小限のアクセス許可が必要です。これらのアクセス許可により、AWS アカウント の AWS WA Tool リソースの詳細をリストおよび表示できます。最小限の必要なアクセス許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しなくなります。

これらのエンティティが AWS WA Tool コンソールを使用できるように、エンティティに次の AWS 管理ポリシーもアタッチします。

```
WellArchitectedConsoleReadOnlyAccess
```

ワークロードを作成、変更、および削除するためには、次の AWS 管理ポリシーをエンティティにアタッチします。

```
WellArchitectedConsoleFullAccess
```

詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

## ユーザーが自分の許可を表示できるようにする

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI か AWS API を使用してプログラム的に、このアクションを完了するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

## ワークロードへのフルアクセスの付与

この例では、ユーザーにワークロードへの AWS アカウント のフルアクセスを許可します。フルアクセスにより、ユーザーは AWS WA Tool ですべてのアクションを実行できます。このアクセスは、ワークロードの定義、ワークロードの削除、ワークロードの表示、ワークロードの更新に必要です。

JSON

```
{
   "Version":"2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:*"
     ],
     "Resource": "*"
     }
   ]
}
```

## ワークロードへの読み取り専用アクセスの付与

この例では、ユーザーにワークロードへの AWS アカウント の読み取り専用アクセスを許可します。読み取り専用アクセスでは、ユーザーは AWS WA Tool のワークロードを表示できるのみです。

JSON

```
{
   "Version":"2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:Get*",
          "wellarchitected:List*"
     ],
     "Resource": "*"
     }
   ]
```

```
}
```

### 1 つのワークロードへのアクセス

この例では、ユーザーに、us-west-2 リージョン内の 1 つのワークロードである 99999999999955555555555566666666 への AWS アカウント の読み取り専用アクセス許可を付与します。お客様の アカウント ID は です777788889999

JSON

```
{
   "Version":"2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:Get*",
          "wellarchitected:List*"
     ],
     "Resource": "arn:aws:wellarchitected:us-
west-2:777788889999:workload/99999999999955555555555566666666"
     }
   ]
}
```

### AWS Well-Architected Tool Connector for Jira のサービス固有の条件キーの使用

この例では、サービス固有の条件キー wellarchitected:JiraProjectKey を使用して、アカウント内のワークロードにリンクできる Jira プロジェクトを制御する方法を示します。

ここでは、条件キーが次のように使用されます。

- **CreateWorkload:** wellarchitected:JiraProjectKey を CreateWorkload に適用すると、ユーザーが作成したワークロードにリンクできるカスタム Jira プロジェクトを定義できます。例えば、ユーザーがプロジェクト ABC で新しいワークロードを作成しようとしても、ポリシーでプロジェクト PQR のみが指定されていると、アクションは拒否されます。
- **UpdateWorkload:** wellarchitected:JiraProjectKey を UpdateWorkload に適用すると、この特定のワークロードまたは任意のワークロードにリンクできるカスタム Jira プロジェク

トを定義できます。例えば、ユーザーがプロジェクト ABC で既存のワークロードを更新しようとしても、ポリシーでプロジェクト PQR が指定されていると、アクションは拒否されます。さらに、プロジェクト PQR にリンクされたワークロードがあり、そのワークロードを更新してプロジェクト ABC にリンクしようとした場合も、アクションは拒否されます。

- **UpdateGlobalSettings:** `wellarchitected:JiraProjectKey` を `UpdateGlobalSettings` に適用すると、AWS アカウントにリンクできるカスタム Jira プロジェクトを定義できます。アカウントレベルの設定は、アカウント内の、アカウントレベルの Jira 設定を上書きしないワークロードを保護します。例えば、ユーザーが `UpdateGlobalSettings` にアクセスした場合、ポリシーで指定されていないプロジェクトにアカウント内のワークロードをリンクすることはできません。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "wellarchitected:UpdateGlobalSettings",
    "wellarchitected:CreateWorkload"
   ],
   "Resource": "*",
   "Condition": {
    "StringEqualsIfExists": {
     "wellarchitected:JiraProjectKey": ["ABC, PQR"]
    }
   }
  },
  {
   "Sid": "VisualEditor1",
   "Effect": "Allow",
   "Action": [
    "wellarchitected:UpdateWorkload"
   ],
   "Resource": "arn:aws:wellarchitected:us-east-1:111122223333:workload/example-workload",
   "Condition": {
    "StringEqualsIfExists": {
```

```
      "wellarchitected:JiraProjectKey": ["ABC, PQR"]
     }
    }
   }
  ]
}
```

## AWS の マネージドポリシーAWS Well-Architected Tool

AWS マネージドポリシーは、AWS が作成および管理するスタンドアロンポリシーです。AWS マネージドポリシーは、多くの一般的なユースケースに対してアクセス許可を提供するように設計されているため、ユーザー、グループ、ロールへのアクセス許可の割り当てを開始できます。

AWS マネージドポリシーは、ご利用の特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることにご注意ください。これは、すべての AWS ユーザーが使用できるようになるのを避けるためです。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS マネージドポリシーで定義されたアクセス許可は変更できません。AWS が AWS マネージドポリシーに定義されているアクセス許可を更新すると、更新はポリシーがアタッチされているすべてのプリンシパルアイデンティティ (ユーザー、グループ、ロール) に影響します。新しい AWS のサービス を起動するか、既存のサービスで新しい API オペレーションが使用可能になると、AWS が AWS マネージドポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

### AWS マネージドポリシー: WellArchitectedConsoleFullAccess

`WellArchitectedConsoleFullAccess` ポリシーを IAM IDにアタッチできます。

このポリシーは、AWS Well-Architected Tool へのフルアクセスを許可します。

アクセス許可の詳細

JSON

```
{
   "Version":"2012-10-17",
   "Statement" : [
```

```
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:*"
     ],
     "Resource": "*"
     }
   ]
}
```

## AWS マネージドポリシー: WellArchitectedConsoleReadOnlyAccess

`WellArchitectedConsoleReadOnlyAccess` ポリシーを IAM IDにアタッチできます。

このポリシーは、AWS Well-Architected Tool に読み取り専用アクセスを許可します。

アクセス許可の詳細

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wellarchitected:Get*",
                "wellarchitected:List*",
                "wellarchitected:ExportLens"
            ],
            "Resource": "*"
        }
    ]
}
```

## AWS マネージドポリシー: AWSWellArchitectedOrganizationsServiceRolePolicy

`AWSWellArchitectedOrganizationsServiceRolePolicy` ポリシーを IAM IDにアタッチできます。

このポリシーは、AWS Organizations の管理者アクセス許可を付与します。このアクセス許可は AWS Well-Architected Tool と組織の統合をサポートするために必要です。これらのアクセス許可により、組織管理アカウントは AWS WA Tool にリソースを共有できるようになります。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `organizations:ListAWSServiceAccessForOrganization` — AWS サービスアクセスを AWS WA Tool に対して有効化できるかを確認をプリンシパルに許可します。
- `organizations:DescribeAccount` - 組織内のアカウントに関する情報の取得をプリンシパルに許可します。
- `organizations:DescribeOrganization` - 組織設定に関する情報の取得を、プリンシパルに許可します。
- `organizations:ListAccounts` - 組織に属するアカウントリストの取得を、プリンシパルに許可します。
- `organizations:ListAccountsForParent` - 組織に属するアカウントのリストを組織の指定ルートノードから取得することをプリンシパルに許可します。
- `organizations:ListChildren` - 組織に属するアカウントのリストの組織部門を組織の指定ルートノードから取得することをプリンシパルに許可します。
- `organizations:ListParents` - 組織内の OU またはアカウントで指定された直属の親リストの取得をプリンシパルに許可します。
- `organizations:ListRoots` - 組織内のすべてのルートノードの一覧の取得をプリンシパルに許可します。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
```

```
                "organizations:ListAccountsForParent",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:ListRoots"
            ],
            "Resource": "*"
        }
    ]
}
```

## AWS マネージドポリシー: AWSWellArchitectedDiscoveryServiceRolePolicy

`AWSWellArchitectedDiscoveryServiceRolePolicy` ポリシーを IAM IDにアタッチできます。

このポリシーにより、AWS Well-Architected Tool は、AWS サービスおよび AWS WA Tool リソースに関連するリソースにアクセスできるようになります。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `trustedadvisor:DescribeChecks` — 利用可能な Trusted Advisor チェックを一覧表示します。
- `trustedadvisor:DescribeCheckItems` — Trusted Advisor がフラグを付けたステータスおよびリソースを含む Trusted Advisor チェックデータをフェッチします。
- `servicecatalog:GetApplication` — AppRegistry アプリケーションの詳細をフェッチします。
- `servicecatalog:ListAssociatedResources` — AppRegistry アプリケーションに関連するリソースを一覧表示します。
- `cloudformation:DescribeStacks` — CloudFormation スタックの詳細を取得します。
- `cloudformation:ListStackResources` — CloudFormation スタックに関連するリソースを一覧表示します。
- `resource-groups:ListGroupResources` — ResourceGroup のリソースを一覧表示します。
- `tag:GetResources` — ListGroupResources には必須。
- `servicecatalog:CreateAttributeGroup` — 必要に応じてサービス管理属性グループを作成します。

- servicecatalog:AssociateAttributeGroup — サービス管理属性グループを AppRegistry アプリケーションに関連付けます。
- servicecatalog:UpdateAttributeGroup — サービス管理属性グループを更新します。
- servicecatalog:DisassociateAttributeGroup — AppRegistry アプリケーションからサービス管理属性グループの関連性を解除します。
- servicecatalog:DeleteAttributeGroup — 必要に応じてサービス管理属性グループを削除します。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeChecks",
    "trustedadvisor:DescribeCheckItems"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "cloudformation:DescribeStacks",
    "cloudformation:ListStackResources",
    "resource-groups:ListGroupResources",
    "tag:GetResources"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "servicecatalog:ListAssociatedResources",
    "servicecatalog:GetApplication",
```

```
      "servicecatalog:CreateAttributeGroup"
     ],
     "Resource": [
      "*"
     ]
    },
    {
     "Effect": "Allow",
     "Action": [
      "servicecatalog:AssociateAttributeGroup",
      "servicecatalog:DisassociateAttributeGroup"
     ],
     "Resource": [
      "arn:*:servicecatalog:*:*:/applications/*",
      "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
     ]
    },
    {
     "Effect": "Allow",
     "Action": [
      "servicecatalog:UpdateAttributeGroup",
      "servicecatalog:DeleteAttributeGroup"
     ],
     "Resource": [
      "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
     ]
    }
   ]
}
```

## AWS WA Tool による AWS マネージドポリシーの更新

このサービスがこれらの変更の追跡を開始してからの、AWS WA Tool の AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動通知については、[AWS WA Tool ドキュメント履歴] ページの RSS フィードをサブスクライブします。

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| AWS WA Tool マネージドポリシーの変更 | `"wellarchitected:Export*"` が `WellArchitectedConsoleRead0` | 2023 年 6 月 22 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| | nlyAccess に追加されました。 | |
| AWS WA Tool が追加したサービスロールポリシー | AWSWellArchitectedDiscoveryServiceRolePolicy を追加すると、AWS Well-Architected Tool が AWS サービスおよび AWS WA Tool リソースに関連するリソースにアクセスできるようになります。 | 2023 年 5 月 3 日 |
| AWS WA Tool が追加したアクセス許可 | AWS サービスアクセスが AWS WA Tool に対して有効になっているかどうかを AWS WA Tool が確認できるよう ListAWSServiceAccessForOrganization に許可する新しいアクションを追加しました。 | 2022 年 7 月 22 日 |
| AWS WA Tool は変更の追跡を開始しました | AWS WA Tool が AWS マネージドポリシーの変更の追跡を開始しました。 | 2022 年 7 月 22 日 |

## AWS Well-Architected Tool ID とアクセスのトラブルシューティング

次の情報は、AWS WA Tool と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修正に役立ちます。

トピック

- でアクションを実行する権限がありませんAWS WA Tool

でアクションを実行する権限がありませんAWS WA Tool

AWS マネジメントコンソール から、アクションを実行する権限がないと通知された場合は、管理者に問い合わせてサポートを依頼する必要があります。管理者とは、サインイン認証情報を提供した担当者です。

以下の例のエラーは、*mateojackson* ユーザーがコンソールを使用して、DeleteWorkload アクションを実行しようとしたが、アクセス許可がない場合に発生します。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: wellarchitected:DeleteWorkload on resource: 11112222333344445555666677778888
```

この例の場合は、wellarchitected:DeleteWorkload アクションを使用して 11112222333344445555666677778888 リソースへのアクセスを許可するように、管理者にポリシーを更新してもらいます。

# AWS Well-Architected Tool でのインシデント対応

AWS Well-Architected Tool に対するインシデント対応は、AWS の責任事項です。AWS には、インシデント対応を管理する正式な文書化されたポリシーとプログラムがあります。

広範な影響を与える AWS の運用上の問題は AWS Service Health Dashboard に投稿されます。

運用上の問題も、AWS Health Dashboard を介して個々のアカウントに投稿されます。Health Dashboard の使い方については、「AWS Health ユーザーガイド」を参照してください。

# AWS Well-Architected Tool のコンプライアンス検証

AWS のサービスが特定のコンプライアンスプログラムの対象であるかどうかを確認するには、「コンプライアンスプログラムによる対象範囲内の AWS のサービス」を参照して、関心のあるコンプライアンスプログラムを選択してください。一般的な情報については、AWSコンプライアンスプログラム を参照してください。

AWS Artifact を使用して、サードパーティの監査レポートをダウンロードできます。詳細については、「AWS Artifact でレポートをダウンロードする」「」を参照してください。

AWS のサービスを使用する際のお客様のコンプライアンス責任は、お客様のデータの機密性や貴社のコンプライアンス目的、適用可能な法律および規制によって決定されます。AWS のサービス を使

用する際のコンプライアンス責任の詳細については、「AWS セキュリティドキュメント」を参照してください。

## AWS Well-Architected Tool の耐障害性

AWS グローバルインフラストラクチャは AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。AWS リージョン は、低レイテンシー、高スループット、そして高度な冗長ネットワークで接続される物理的に独立、隔離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャに比べて、可用性、耐障害性、および拡張性に優れています。

AWS リージョン とアベイラビリティーゾーンの詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

## AWS Well-Architected Tool でのインフラストラクチャセキュリティ

マネージドサービスである AWS Well-Architected Tool は AWS グローバルネットワークセキュリティで保護されています。AWSセキュリティサービスと AWS がインフラストラクチャを保護する方法については、「AWSクラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、セキュリティの柱 - AWS Well-Architected Frameworkのインフラストラクチャ保護を参照してください。

AWS の発行済み API コールを使用して、ネットワーク経由で AWS WA Tool にアクセスします。クライアントは次をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは Java 7 以降など、ほとんどの最新システムでサポートされています。

## AWS Well-Architected Tool での設定と脆弱性の分析

構成および IT 管理は、AWS、お客様および弊社のお客様の間で共有される責任です。詳細については、「AWS 責任共有モデル」を参照してください。

# サービス間の混乱した代理の防止

混乱した代理問題は、アクションを実行する許可を持たないエンティティが、より特権のあるエンティティにアクションを実行するように強制できるセキュリティの問題です。AWS では、サービス間でのなりすましによって、混乱した代理問題が発生する場合があります。サービス間でのなりすましは、1 つのサービス (呼び出し元サービス) が、別のサービス (呼び出し対象サービス) を呼び出すときに発生する可能性があります。呼び出し元サービスは、本来ならアクセスすることが許可されるべきではない方法でその許可を使用して、別のお客様のリソースに対する処理を実行するように操作される場合があります。これを防ぐため、AWS では、アカウント内のリソースへのアクセス権が付与されたサービスプリンシパルですべてのサービスのデータを保護するために役立つツールを提供しています。

リソースポリシーで aws:SourceArn および aws:SourceAccount のグローバル条件コンテキストキーを使用して、AWS Well-Architected Tool が別のサービスに付与する許可をそのリソースに制限することをお勧めします。クロスサービスアクセスにリソースを 1 つだけ関連付けたい場合は、aws:SourceArn を使用します。そのアカウント内のリソースをクロスサービスの使用に関連付けることを許可する場合は、aws:SourceAccount を使用します。

混乱した代理問題から保護するための最も効果的な方法は、リソースの完全な ARN を指定して、aws:SourceArn グローバル条件コンテキストキーを使用することです。リソースの完全な ARN が不明な場合や、複数のリソースを指定する場合には、グローバルコンテキスト条件キー aws:SourceArn で、ARN の未知部分を示すためにワイルドカード文字 (*) を使用します。例えば、arn:aws:wellarchitected:*:*123456789012*:*。

aws:SourceArn の値に Amazon S3 バケット ARN などのアカウント ID が含まれていない場合は、両方のグローバル条件コンテキストキーを使用して、アクセス許可を制限する必要があります。

aws:SourceArn の値はワークロードかレンズにする必要があります。

次の例では、AWS WA Tool で aws:SourceArn および aws:SourceAccount グローバル条件コンテキストキーを使用して、混乱した代理問題を回避する方法を示します。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
```

```
    "Principal": {
      "Service": "wellarchitected.amazonaws.com"
    },
    "Action": "wellarchitected:CreateWorkload",
    "Resource": [
    "arn:aws:wellarchitected:us-east-1:111122223333:ResourceName/*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:wellarchitected:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

# AWS WA Tool リソースの共有

所有しているリソースを共有するには、次の手順を実行します。

- AWS Organizations 内でリソース共有を有効にする (オプション)
- ワークロードを共有する
- カスタムレンズを共有する
- プロフィールを共有する
- レビューテンプレートを共有する

> **注意事項**
>
> - リソースを共有すると、そのリソースを作成した AWS アカウント 以外のプリンシパルもそれを使用できるようになります。共有しても、リソースを作成したアカウントのリソースに適用されるアクセス許可は変わりません。
> - AWS WA Tool はリージョンサービスです。共有先のプリンシパルは、リソース共有が作成された AWS リージョン 内のみのアクセスが可能です。
> - 2019 年 3 月 20 日以降に開設されたリージョンでリソースを共有するには、自分と共有済みの AWS アカウント の両方が AWS マネジメントコンソール でそのリージョンを有効にする必要があります。詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

## AWS Organizations 内でリソース共有を有効にする

アカウントが AWS Organizations によって管理されている場合、それを活用すればリソースを共有しやすくなります。組織の有無にかかわらず、ユーザーは個々のアカウントに共有できます。ただし、アカウントが組織内にある場合には、各アカウントを列挙しなくても、個々のアカウント、または組織内または OU 内のすべてのアカウントとの共有が可能です。

組織内でリソースを共有するには、まず AWS WA Tool コンソールまたは AWS Command Line Interface (AWS CLI) を使用して AWS Organizations との共有を有効にする必要があります。組織内でリソースを共有する場合、AWS WA Tool はプリンシパルに招待を送信しません。組織内のプリンシパルは、招待状を交換せずに共有リソースにアクセスできます。

組織内でリソースの共有を有効にする場合、AWS WA Tool は `AWSServiceRoleForWellArchitected` と呼ばれるサービスがリンクされたロールを作成します。このロールは AWS WA Tool サービスのみに適用でき、AWS マネージドポリシー `AWSWellArchitectedOrganizationsServiceRolePolicy` を使用して、そのサービスが所属する組織に関する情報を取得する AWS WA Tool アクセス許可を付与します。

組織全体または OU とリソースを共有する必要がなくなった場合は、リソース共有を無効にできます。

要件

- これらの手順は、組織の管理アカウントのプリンシパルとしてサインインしている場合のみ実行できます。
- その組織で、すべての機能が有効になっている必要があります。詳細については、「AWS Organizations ユーザーガイド」の「組織内のすべての機能の有効化」を参照してください。

> **Important**
>
> AWS WA Tool コンソールを使用して AWS Organizations との共有を有効にする必要があります。これにより、`AWSServiceRoleForWellArchitected` サービスにリンクされたロールが確実に作成されます。AWS Organizations コンソールまたは enable-aws-service-access AWS CLI コマンドを使用して AWS Organizations への信頼されたアクセスを有効にすると、`AWSServiceRoleForWellArchitected` サービスにリンクされたロールが作成されず、組織内でリソースを共有できなくなります。

組織内でリソース共有を有効にするには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool コンソールを開きます。

   組織の管理アカウントのプリンシパルとしてサインインしている必要があります。
2. 左側のナビゲーションペインの [設定] を選択します。
3. [AWS Organizations のサポートを有効化] を選択します。
4. [設定を保存] を選択します。

### 組織内でリソース共有を無効にするには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool コンソールを開きます。

   組織の管理アカウントのプリンシパルとしてサインインしている必要があります。
2. 左側のナビゲーションペインの [設定] を選択します。
3. [AWS Organizations のサポートを有効化] を選択解除します。
4. [設定を保存] を選択します。

# AWS WA Tool リソースのタグ付け

AWS WA Tool リソースを管理しやすくするために、タグ形式で各リソースに独自のメタデータを割り当てることができます。ここではタグとその作成方法について説明します。

内容



## タグの基本

タグとはAWS リソースに割り当てるラベルです。タグはそれぞれ、1 つのキーとオプションの 1 つの値で構成されており、どちらもお客様側が定義します。

タグを使用すると、AWS リソースを目的、所有者、環境などで分類できます。同じ型のリソースが多い場合に、割り当てたタグに基づいて特定のリソースをすばやく識別できます。たとえば、AWS WA Tool サービスに一連のタグを定義して、各サービスの所有者とスタックレベルを追跡できます。リソースタイプごとに一貫した一連のタグキーを考案することをお勧めします。

タグは自動的にはリソースに割り当てられません。タグを追加したら、いつでもタグキーと値は編集でき、タグはリソースからいつでも削除できます。リソースを削除すると、リソースのタグも削除されます。

タグには、AWS WA Tool に関連する意味はなく、完全に文字列として解釈されます。タグの値を空の文字列に設定することはできますが、タグの値を null に設定することはできません。特定のリソースについて既存のタグと同じキーを持つタグを追加した場合、以前の値は新しい値によって上書きされます。

AWS マネジメントコンソール、AWS CLI、および AWS WA Tool API を使用してタグを操作できます。

AWS Identity and Access Management (IAM) を使用している場合は、タグを作成、編集、削除するためのアクセス許可を持つ AWS アカウントのユーザーを制御できます。

# リソースのタグ付け

新しいまたは既存の AWS WA Tool リソースにタグを付けることができます。

AWS WA Tool コンソールを使用している場合、新しいリソースには作成時にタグを適用でき、既存のリソースにはいつでもタグを適用できます。既存のワークロードには、[プロパティ] タブからタグを適用できます。既存のカスタムレンズ、プロファイル、レビューテンプレートには、[概要] タブからタグを適用できます。

AWS WA Tool API、AWS CLI、または AWS SDK を使用している場合、新しいリソースには、関連する API アクションの `tags` パラメータを使用してタグを適用でき、既存のリソースには、`TagResource` API アクションを使用してタグを適用できます。詳細については、「TagResource」を参照してください。

リソース作成アクションによっては、リソースの作成時にリソースのタグを指定できます。リソースの作成時にタグを適用できない場合、リソースの作成プロセスは失敗します。これにより、作成時にタグ付けするリソースが、指定したタグで作成されるか、まったく作成されないことが確認されます。作成時にリソースにタグを付ける場合、リソースの作成後にカスタムのタグ付けスクリプトを実行する必要はありません。

次の表では、タグ付け可能な AWS WA Tool リソースと、作成時にタグ付け可能なリソースについて説明します。

AWS WA Tool リソースのタグ付けのサポート

| リソース | タグをサポート | タグの伝播をサポート | 作成時のタグ付けをサポート (AWS WA Tool API、AWS CLI、AWS SDK) |
|---|---|---|---|
| AWS WA Tool ワークロード | はい | なし | あり |
| AWS WA Tool カスタムレンズ | はい | なし | あり |
| AWS WA Tool プロファイル | はい | なし | あり |

| リソース | タグをサポート | タグの伝播をサポート | 作成時のタグ付けをサポート (AWS WA Tool API、AWS CLI、AWS SDK) |
| --- | --- | --- | --- |
| AWS WA Tool レビューテンプレート | はい | なし | あり |

# タグの制限

タグには以下のような基本制限があります。

- リソースあたりのタグの最大数 - 50 件
- タグキーはリソースごとにそれぞれ一意である必要があります。また、各タグキーに設定できる値は 1 つのみです。
- キーの最大長 - UTF-8 の 128 Unicode 文字
- 値の最大長 - UTF-8 の 256 Unicode 文字
- 複数の AWS サービス間およびリソース間でタグ付けスキーマを使用する場合、他のサービスでも許可される文字に制限が適用されることがあるのでご注意ください。一般的に使用が許可される文字は、UTF-8 で表現できる文字、数字、スペース、および +、-、=、.、_、:、/、@。
- タグのキーと値では、大文字と小文字が区別されます。
- `aws:`、`AWS:`、またはその大文字または小文字の組み合わせを、キーまたは値のプレフィックスとして使用しないでください。これらの文字列は AWS による使用のために予約されています。このプレフィックスを持つタグのキーや値を編集または削除することはできません。このプレフィックスを持つタグは、リソースあたりのタグ数の制限時には計算されません。

# コンソールでのタグの処理

AWS WA Tool コンソールを使用すると、新しいリソースまたは既存のリソースに関連付けられたタグを管理できます。

## 作成時に個々のリソースにタグを追加する

リソースを作成時に AWS WA Tool リソースにタグを追加できます。

# 個々のリソースでタグを追加および削除する

AWS WA Tool を使用すると、ワークロードの [プロパティ] タブおよびカスタムレンズ、プロファイル、レビューテンプレートの [概要] タブから直接リソースに関連付けられているタグを追加または削除できます。

ワークロードのタグを追加または削除するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [Workloads] (ワークロード) を選択します。
4. 修正するワークロードを選択し、[Properties] (プロパティ) を選択します。
5. [タグ] セクションで、[タグを管理] を選択します。
6. 必要に応じてタグを追加または削除します。
   - タグを追加するには、[Add new tag] (新しいタグの追加) を選択し、[Key] (キー) と [Value] (値) のフィールドに入力します。
   - タグを削除するには、[削除] を選択します。
7. 追加、変更、削除を行うタグごとにこのプロセスを繰り返します。[保存] を選択して変更を保存します。

カスタムレンズのタグを追加または削除するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [カスタムレンズ] を選択します。
4. 変更するカスタムレンズの名前を選択します。
5. [概要] タブの [タグ] セクションで、[タグを管理] を選択します。
6. 必要に応じてタグを追加または削除します。
   - タグを追加するには、[Add new tag] (新しいタグの追加) を選択し、[Key] (キー) と [Value] (値) のフィールドに入力します。
   - タグを削除するには、[削除] を選択します。

7. 追加、変更、削除を行うタグごとにこのプロセスを繰り返します。[保存] を選択して変更を保存します。

プロファイルでタグを追加または削除するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [プロファイル] を選択します。
4. 修正するプロファイルの名前を選択します。
5. [概要] タブの [タグ] セクションで、[タグを管理] を選択します。
6. 必要に応じてタグを追加または削除します。
   - タグを追加するには、[Add new tag] (新しいタグの追加) を選択し、[Key] (キー) と [Value] (値) のフィールドに入力します。
   - タグを削除するには、[削除] を選択します。
7. 追加、変更、削除を行うタグごとにこのプロセスを繰り返します。[保存] を選択して変更を保存します。

レビューテンプレートでタグを追加または削除するには

1. AWS マネジメントコンソール にサインインし、https://console.aws.amazon.com/wellarchitected/ で AWS Well-Architected Tool のコンソールを開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [レビューテンプレート] を選択します。
4. 変更するレビューテンプレートの名前を選択します。
5. [概要] タブの [タグ] セクションで、[タグを管理] を選択します。
6. 必要に応じてタグを追加または削除します。
   - タグを追加するには、[Add new tag] (新しいタグの追加) を選択し、[Key] (キー) と [Value] (値) のフィールドに入力します。
   - タグを削除するには、[削除] を選択します。
7. 追加、変更、削除を行うタグごとにこのプロセスを繰り返します。[保存] を選択して変更を保存します。

# API を使用したタグの操作

リソースのタグの追加、更新、リスト表示、および削除には、次の AWS WA Tool API オペレーションを使用します。

AWS WA Tool リソースのタグ付けのサポート

| タスク | API アクション |
| --- | --- |
| 1 つ以上のタグを追加、または上書きします。 | TagResource |
| 1 つ以上のタグを削除します。 | UntagResource |
| リソースのタグを一覧表示します。 | ListTagsForResource |

一部のリソース作成アクションでは、リソースの作成時にタグを指定できます。以下のアクションでは、作成時のタグ付けがサポートされます。

| タスク | API アクション |
| --- | --- |
| ワークロードの作成 | CreateWorkload |
| 新しいレンズをインポートする | ImportLens |
| プロファイルを作成する | CreateProfile |
| レビューテンプレートを作成する | CreateReviewTemplate |

# AWS WA Tool による AWS CloudTrail API コールのログ記録

AWS Well-Architected Tool は AWS CloudTrail という、AWS WA Tool の ユーザー、ロール、または AWS のサービスが実行したアクションを記録するサービスと統合しています。CloudTrail は、AWS WA Tool のすべての API コールをイベントとしてキャプチャします。キャプチャされたコールには、AWS WA Tool コンソールのコールと、AWS WA Tool API オペレーションへのコードのコールが含まれます。証跡を作成する場合は、AWS WA Tool のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます 証跡を設定しない場合でも、「CloudTrail」 コンソールの 「イベント履歴」 で最新のイベントを表示できます。CloudTrail が収集した情報を使用して、AWS WA Tool に対して行われた要求、要求が行われた IP アドレス、要求を行った人、要求が行われた日時、および追加の詳細を判別できます。

CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

## CloudTrail での AWS WA Tool 情報

CloudTrail は、アカウント作成時に AWS アカウント で有効になります。AWS WA Tool でアクティビティが発生すると、そのアクティビティは [Event history] (イベント履歴) の他の AWS のサービスのイベントとともに CloudTrail イベントに記録されます。最近のイベントは、AWS アカウント で表示、検索、ダウンロードできます。詳細については、「CloudTrail イベント履歴でのイベントの表示」を参照してください。

AWS WA Tool のイベントなど、AWS アカウント のイベントの継続的な記録に対して、追跡を作成します。追跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョン に適用されます。証跡は、AWS パーティションのすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集したイベントデータをより詳細に分析し、それに基づいて対応するため、他の AWS サービスを構成できます。詳細については、次を参照してください:

- 証跡の作成のための概要
- CloudTrail がサポートするサービスと統合
- CloudTrail 用 Amazon SNS 通知の構成
- [複数のリージョンから CloudTrail ログファイルを受け取る] および [複数のアカウントから CloudTrail ログファイルを受け取る]

すべての AWS WA Tool アクションは CloudTrail によってログに記録され、AWS Well-Architected Toolで定義されたアクションに記録されます。例えば、CreateWorkload、DeleteWorkload、CreateWorkloadShare の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- ユーザーまたはルートユーザーの認証情報のどちらを使用してリクエストが送信されたか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、「CloudTrail userIdentity 要素」を参照してください。

## AWS WA Tool ログファイルエントリの理解

追跡は、指定したAmazon S3バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどの情報を含みます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

以下の例は、CreateWorkload アクションを示す CloudTrail ログエントリです。

```
   {
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:dev-dsk-xiulan-2a-1111111c.us-
west-2.amazon.com",
        "arn": "arn:aws:sts::444455556666:assumed-role/well-architected-api-svc-integ-
test-read-write/dev-dsk-xiulan-2a-1111111c.us-west-2.amazon.com",
        "accountId": "444455556666",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
```

```
                "arn": "arn:aws:iam::444455556666:role/well-architected-api-svc-integ-
test-read-write",
                "accountId": "444455556666",
                "userName": "well-architected-api-svc-integ-test-read-write"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-10-14T03:41:39Z"
            }
        }
    },
    "eventTime": "2020-10-14T04:43:13Z",
    "eventSource": "wellarchitected.amazonaws.com",
    "eventName": "CreateWorkload",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.178",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.848
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.262-b10
 java/1.8.0_262 vendor/Oracle_Corporation",
    "requestParameters": {
           "ClientRequestToken": "08af866a-0238-4070-89c2-b689ca8339f7",
           "Description": "***",
           "AwsRegions": [
               "us-west-2"
           ],
           "ReviewOwner": "***",
           "Environment": "PRODUCTION",
           "Name": "***",
           "Lenses": [
               "wellarchitected",
               "serverless"
           ]
    },
    "responseElements": {
         "Arn": "arn:aws:wellarchitected:us-
west-2:444455556666:workload/8cdcdf7add10b181fdd3f686dacffdac",
         "Id": "8cdcdf7add10b181fdd3f686dacffdac"
    },
    "requestID": "22bad4e3-aa51-4ff1-b480-712ee07cedbd",
    "eventID": "50849dfd-36ed-418e-a901-49f6ac7087e8",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
```

```
}
```

# EventBridge

Well-Architected リソースに対してアクションが実行されると、AWS Well-Architected Tool は、Amazon EventBridge にイベントを送信します。EventBridge およびこれらのイベントを使用すると、リソースが変更されたときに通知を送信するなどのアクションを実行するルールを記述できます。詳細については、「Amazon EventBridge とは」を参照してください。

> **Note**
>
> イベントは、ベストエフォートベースで送信されます。

次のアクションにより、EventBridge イベントが発生します。

- ワークロード関連
  - ワークロードの作成または削除
  - マイルストーンの作成
  - ワークロードのプロパティの更新
  - ワークロードの共有または共有解除
  - 共有の招待ステータスの更新
  - タグの追加と削除
  - 回答の更新
  - レビューノートの更新
  - ワークロードからのレンズの追加または削除
- レンズ関連
  - カスタムレンズのインポートまたはエクスポート
  - カスタムレンズの公開
  - カスタムレンズの削除
  - カスタムレンズの共有または共有解除
  - 共有の招待ステータスの更新
  - ワークロードからのレンズの追加または削除

# AWS WA Tool からのイベント例

このセクションでは、AWS Well-Architected Tool からのイベント例を示します。

## ワークロード内の回答の更新


```
{
  "version":"0",
  "id":"00de336a-83cc-b80b-f0e6-f44c88a96050",
  "detail-type":"AWS API Call via CloudTrail",
  "source":"aws.wellarchitected",
  "account":"123456789012",
  "time":"2022-02-17T08:01:25Z",
  "region":"us-west-2",
  "resources":[],
  "detail":{
     "eventVersion":"1.08",
     "userIdentity":{
        "type":"AssumedRole",
        "principalId":"AROA4JUSXMN5ZR6S7LZNP:sample-user",
        "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "sessionContext":{
           "sessionIssuer":{
              "type":"Role",
              "principalId":"AROA4JUSXMN5ZR6S7LZNP",
              "arn":"arn:aws:iam::123456789012:role/Admin",
              "accountId":"123456789012",
              "userName":"Admin"
           },
           "webIdFederationData":{},
           "attributes":{
              "creationDate":"2022-02-17T07:21:54Z",
              "mfaAuthenticated":"false"
           }
        }
     },
     "eventTime":"2022-02-17T08:01:25Z",
     "eventSource":"wellarchitected.amazonaws.com",
     "eventName":"UpdateAnswer",
     "awsRegion":"us-west-2",
```

```
      "sourceIPAddress":"10.246.162.39",
      "userAgent":"aws-internal/3 aws-sdk-java/1.12.127
 Linux/5.4.156-94.273.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07
 java/1.8.0_312 vendor/Oracle_Corporation cfg/retry-mode/standard",
      "requestParameters":{
         "Status":"Acknowledged",
         "SelectedChoices":"***",
         "ChoiceUpdates":"***",
         "QuestionId":"priorities",
         "WorkloadId":"ee73fda518f9bd4aa804c6252e4e37b0",
         "IsApplicable":true,
         "LensAlias":"wellarchitected",
         "Reason":"NONE",
         "Notes":"***"
      },
      "responseElements":{
         "Answer":"***",
         "LensAlias":"wellarchitected",
         "WorkloadId":"ee73fda518f9bd4aa804c6252e4e37b0"
      },
      "requestID":"7bae1153-26a8-4dc0-9307-68b17b107619",
      "eventID":"8339c258-4ddd-48aa-ab21-3f82ce9d79cd",
      "readOnly":false,
      "eventType":"AwsApiCall",
      "managementEvent":true,
      "recipientAccountId":"123456789012",
      "eventCategory":"Management"
   }
}
```

## カスタムレンズの公開

```
{
   "version":"0",
   "id":"4054a34b-60a9-53c1-3146-c1a384dba41b",
   "detail-type":"AWS API Call via CloudTrail",
   "source":"aws.wellarchitected",
   "account":"123456789012",
   "time":"2022-02-17T08:58:34Z",
   "region":"us-west-2",
   "resources":[],
```

```
   "detail":{
      "eventVersion":"1.08",
      "userIdentity":{
         "type":"AssumedRole",
         "principalId":"AROA4JUSXMN5ZR6S7LZNP:example-user",
         "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
         "accountId":"123456789012",
         "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
         "sessionContext":{
            "sessionIssuer":{
               "type":"Role",
               "principalId":"AROA4JUSXMN5ZR6S7LZNP",
               "arn":"arn:aws:iam::123456789012:role/Admin",
               "accountId":"123456789012",
               "userName":"Admin"
            },
            "webIdFederationData":{},
            "attributes":{
               "creationDate":"2022-02-17T07:21:54Z",
               "mfaAuthenticated":"false"
            }
         }
      },
      "eventTime":"2022-02-17T08:58:34Z",
      "eventSource":"wellarchitected.amazonaws.com",
      "eventName":"CreateLensVersion",
      "awsRegion":"us-west-2",
      "sourceIPAddress":"10.246.162.39",
      "userAgent":"aws-internal/3 aws-sdk-java/1.12.127
 Linux/5.4.156-94.273.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07
 java/1.8.0_312 vendor/Oracle_Corporation cfg/retry-mode/standard",
      "requestParameters":{
         "IsMajorVersion":true,
         "LensVersion":"***",
         "ClientRequestToken":"03f46163-e95c-4455-8479-266373aa09c7",
         "LensAlias":"***"
      },
      "responseElements":{
         "LensArn":"arn:aws:wellarchitected:us-
west-2:123456789012:lens/6261deecb9def44f9aecc938ca25d94e",
         "LensVersion":"***"
      },
      "requestID":"167b7051-980d-42ee-9967-0b4b3163e948",
      "eventID":"c7ef2b47-419d-45b7-8982-fbade9b558c7",
```

```
      "readOnly":false,
      "eventType":"AwsApiCall",
      "managementEvent":true,
      "recipientAccountId":"123456789012",
      "eventCategory":"Management"
   }
}
```

# ドキュメントの改訂

次の表は、AWS Well-Architected Tool の今回のリリースのドキュメントをまとめたものです。

- API バージョン: 最新
- ドキュメントの最終更新日: 2025 年 10 月 13 日

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 「Well-Architected フレームワークレビュー (WAFR)」セクション | AWS Well-Architected Tool を使用して WAFR を実行するためのガイダンスが含まれる新しいセクションを追加しました。 | 2025 年 10 月 13 日 |
| 新しいレンズ | このリリースでは、レンズカタログに新しいレンズが 1 つ追加されました。 | 2025 年 4 月 17 日 |
| 新しいレンズと更新されたレンズ | このリリースでは、レンズカタログに新しいレンズが 1 つ追加され、他のレンズが 1 つ更新されました。 | 2024 年 6 月 27 日 |
| Jira | このリリースでは、AWS Well-Architected Tool Connector for Jira が追加されました。 | 2024 年 4 月 16 日 |
| 新しいレンズ | このリリースでは、レンズカタログに新しいレンズが追加されました。 | 2024 年 3 月 26 日 |
| 更新された機能 | このリリースでは、AWS WA Tool にレンズカタログ機能が追加されました。 | 2023 年 11 月 26 日 |

| | | |
|---|---|---|
| 更新された機能 | このリリースでは、AWS WA Tool に [レビューテンプレート] 機能が追加されました。 | 2023 年 10 月 3 日 |
| WellArchitectedConsoleReadOnlyAccess マネージドポリシーを更新 | `"wellarchitected:ExportLens"` が `WellArchitectedConsoleReadOnlyAccess` に追加されました。 | 2023 年 6 月 22 日 |
| 更新された機能 | このリリースでは、AWS WA Tool に [プロファイル] 機能が追加されました。 | 2023 年 6 月 13 日 |
| 更新された機能 | このリリースでは、AWS Trusted Advisor と AWS Service Catalog AppRegistry の統合が強化され、`AWSWellArchitectedDiscoveryServiceRolePolicy` が AWS マネージドポリシーに追加されました。 | 2023 年 5 月 3 日 |
| コンテンツの更新 | [ダッシュボード] ページが更新され、リスクと改善計画の詳細情報が含まれるようになりました。統合ワークロードレポートを作成する機能も追加されました。 | 2023 年 3 月 30 日 |
| コンテンツの更新 | WellArchitectedConsoleReadOnlyAccess ポリシーの名前が修正されました。 | 2023 年 1 月 19 日 |

| | | |
|---|---|---|
| の IAM ガイダンスを更新しましたAWS WA Tool | IAM ベストプラクティスに沿ってガイドを更新しました。詳細については、「IAM のセキュリティのベストプラクティス」を参照してください。 | 2023 年 1 月 4 日 |
| 更新された機能 | このリリースでは、FTR レンズがツールから削除されました。 | 2022 年 12 月 14 日 |
| 更新された機能 | このリリースでは、AWS Trusted Advisor と AWS Service Catalog AppRegistry の統合が追加されました。 | 2022 年 11 月 7 日 |
| コンテンツの更新 | choices のカスタムレンズ JSON の例の問題を修正しました。 | 2022 年 9 月 29 日 |
| コンテンツの更新 | カスタムレンズ JSON 仕様の choices セクションが更新されました。 | 2022 年 8 月 2 日 |
| 更新された機能 | このリリースでは、AWS マネージドポリシーの変更を追跡できる、ListAWSServiceAccessForOrganization アクセス許可を AWSWellArchitectedOrganizationsServiceRolePolicy に付与する新しいアクションが追加されました。 | 2022 年 7 月 22 日 |

| | | |
|---|---|---|
| 組織共有が追加されました | このリリースでは、ワークロードやカスタムレンズを組織や組織部門 (OU) と共有する機能が追加されました。 | 2022 年 6 月 30 日 |
| 更新された機能 | このリリースでは、カスタムレンズの選択肢に追加リソースを指定する機能、公開前にカスタムレンズをプレビューする機能、カスタムレンズにタグを追加する機能が追加されました。 | 2022 年 6 月 21 日 |
| 更新された機能 | このリリースでは、AWS re: POST の AWS Well-Architected コミュニティにアクセスする機能が追加されました。 | 2022 年 5 月 31 日 |
| 更新された機能 | このリリースでは、チュートリアルにサステナビリティの柱とマイナーアップデートが追加されました。 | 2022 年 3 月 31 日 |
| EventBridge サポートを追加 | AWS WA Tool は、Well-Architected リソースが変更されたときにイベントを Amazon EventBridge に送信するようになりました。 | 2022 年 3 月 3 日 |
| 更新された機能 | 個々のベストプラクティスを適用しないものとしてマークできるようになりました。 | 2021 年 7 月 14 日 |
| リソースへのタグ付けが可能に | このリリースでは、ワークロードにタグを追加する機能が追加されました。 | 2021 年 3 月 3 日 |

| | | |
|---|---|---|
| API の提供を開始 | このリリースでは、AWS WA Tool API が追加されました。AWS CloudTrail ログ情報も追加されました。 | 2020 年 12 月 16 日 |
| 更新された機能 | このリリースでは、FTR レンズと SaaS レンズがツールに追加されました。 | 2020 年 12 月 3 日 |
| データ保護の更新 | データ保護情報が更新されました。 | 2020 年 11 月 5 日 |
| コンテンツの更新 | 新しいレンズを使用するようにワークロードをアップグレードした後、以前のバージョンに戻すことはできないことを明確化しました。 | 2020 年 7 月 8 日 |
| コンテンツの更新 | 2019 年 3 月 20 日以降に導入された AWS リージョンでの共有について明確化しました。 | 2020 年 6 月 24 日 |
| 更新された機能 | ワークロード共有への招待が拒否されると、ワークロード共有へのアクセスはすぐに削除されます。共有が承諾されると、共有アクセスが許可されます。 | 2020 年 6 月 17 日 |
| コンテンツの更新 | 高リスクの問題 (HRI) と中リスクの問題 (MRI) の定義を追加しました。 | 2020 年 6 月 12 日 |
| コンテンツの更新 | AWS によるお客様データの使用に関するセクションが追加されました。 | 2020 年 5 月 21 日 |

| | | |
|---|---|---|
| 更新された機能 | このリリースでは、レビュー所有者がワークロードに追加されます。 | 2020 年 4 月 1 日 |
| 更新された機能 | このリリースでは、ワークロードにアーキテクチャ図のリンクが追加されます。 | 2020 年 3 月 10 日 |
| コンテンツの更新 | ワークロード共有が AWS リージョン固有であることを明確化しました。 | 2020 年 1 月 10 日 |
| 更新された機能 | このリリースでは、ワークロードの共有を追加しました。 | 2020 年 1 月 9 日 |
| コンテンツの更新 | セキュリティセクションが最新のガイダンスで更新されました。 | 2019 年 12 月 6 日 |
| 更新された機能 | このリリースでは、ワークロードを定義するときに [業界] フィールドがオプションになります。 | 2019 年 8 月 19 日 |
| 更新された機能 | このリリースでは、ワークロードレポートに改善計画項目が追加されました。 | 2019 年 7 月 29 日 |
| 更新された機能 | このリリースでは、DeleteWorkload アクションがポリシーに追加されました。 | 2019 年 7 月 18 日 |
| コンテンツの更新 | このガイドの内容は、わずかな修正を加えて更新されました。 | 2019 年 6 月 19 日 |

| | | |
|---|---|---|
| コンテンツの更新 | このガイドの内容は、わずかな修正を加えて更新されました。 | 2019 年 5 月 30 日 |
| 更新された機能 | このリリースでは、ワークロードレビューに使用されるフレームワークのバージョンのアップグレードがサポートされました。 | 2019 年 5 月 1 日 |
| 更新された機能 | このリリースでは、ワークロードを定義するときに AWS リージョン以外を指定する機能が追加されました。 | 2019 年 2 月 14 日 |
| AWS Well-Architected Tool の一般提供 | このリリースでは、AWS Well-Architected Tool が導入されました。 | 2018 年 11 月 29 日 |

# AWS 用語集

AWS の最新の用語については、「AWS の用語集リファレンス」の「AWS 用語集」を参照してください。