



セキュリティ情報

AWS Control Catalog



AWS Control Catalog: セキュリティ情報

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

Control Catalog とは	1
オントロジーの概要	1
Control Catalog へのアクセス	3
セキュリティ	4
データ保護	4
データ暗号化	5
転送中の暗号化	6
キー管理	6
ネットワーク間トラフィックのプライバシー	6
ID とアクセス管理	6
オーディエンス	6
アイデンティティを使用した認証	7
ポリシーを使用したアクセスの管理	8
Control Catalog と IAM の連携方法	10
アイデンティティベースのポリシーの例	17
トラブルシューティング	20
コンプライアンス検証	22
耐障害性	22
インフラストラクチャセキュリティ	22
設定と脆弱性	23
モニタリング	24
CloudTrail ログ	24
CloudTrail のコントロールカタログ情報	24
Control Catalog ログファイルエントリについて	25
AWS PrivateLink	27
考慮事項	27
インターフェイスエンドポイントの作成	27
エンドポイントポリシーを作成する	28
ドキュメント履歴	30
.....	xxxi

Control Catalog とは

Control Catalog セキュリティ情報ガイドへようこそ。Control Catalog は の一部であり AWS Control Tower、複数の AWS サービスのコントロールを一覧表示します。これは、コントロールの統合 AWS カタログです。Control Catalog を使用する AWS Control Tower ように をセットアップする必要はありません。

Control Catalog を使用すると、セキュリティ、コスト、耐久性、オペレーションなどの一般的なユースケースに従ってコントロールを表示できます。

このドキュメントでは、Control Catalog が提供する APIs を使用する際に知っておくべきセキュリティおよびコンプライアンス情報を確認できます。

Control Catalog は、コントロールの標準分類システムであるコントロールオントロジーを具体化しています。

オントロジーの概要

AWS は、コントロール間のマッピングの分類、整理、作成に役立つ標準分類システムを開発しました。このオントロジーは、コントロールを 24 のフレームワークを含む既存および新規の規制標準、PCI、HIPAA などの規制標準にマッピングするために使用できます。また、NIST や ISO などの業界標準、および Well-Architected フレームワークを含む Amazon 固有のフレームワークにもマッピングされます。

オントロジーには 4 つの主要な側面があります。

- コントロールドメイン、コントロールの目的、一般的なコントロールによるコントロールの分類。オントロジーは、関連するコントロールを整理して 3 つのレベルにグループ化するのに役立ちます。
 - L1: コントロールドメイン、
 - L2: コントロールの目標、
 - L3: 共通コントロール。

これらのレベルには、厳密な階層関係があります。つまり、各ドメインには複数のコントロール目標がありますが、各コントロール目標には 1 つの親ドメインが必要です。各コントロール目標には複数の共通コントロールがありますが、各共通コントロールには 1 つの親目標があります。

- 規制標準へのマッピング。オントロジーには、規制または業界標準内の特定の要件を表す標準コントロール (L4) と呼ばれる概念があります。これらの標準コントロールは、これらの特定の要件を満たすのに役立つ共通コントロールにマッピングされます。

例えば、PCI-DSS v3.2.1 などです。ID 4.1 強力な暗号化とセキュリティプロトコルを使用して、オープンなパブリックネットワークを介した送信中に機密性の高いカード所有者データを保護します。NIST 800.53.r5 ID SC-16 セキュリティ属性とプライバシー属性の送信は 2 つの標準コントロールであり、どちらも転送中の暗号化データへのマッピング共通コントロールです。

- コントロールの実装とコントロールの証拠。オントロジーには、コントロール実装 (L6) の概念があり、コントロール AWS、AWS Security Hub CSPM チェック、AWS Config ルールなどの特定の AWS Control Tower コントロール実装、またはプロセスガイダンス AWS などの外部での非技術的な実装を表すことができます。コントロール証拠 (L7) の別の概念は、サードパーティーのツール AWS Audit Manager、またはお客様自身によるコントロールの証拠として使用できるデータソースを表します。これらの証拠ソースは、AWS CloudTrail イベント、API コールログ、AWS Config ルール評価結果などの AWS ソースである可能性があります。または、顧客ドキュメントなどの外部ソースである場合もあります。
- Core コントロール (L5) の概念。Core コントロールは、すべてのコントロール実装 (L6)、対応する証拠ソース (L7)、関連する標準コントロール (L4)、共通コントロール (L3) を 1 つの包括的なオブジェクトに統合するマッピングレイヤーです。Core コントロールは、コントロール自体よりもマッピングドキュメントです。これは、コントロール X に関連するすべての情報を表示するという質問に答えるのに役立ちます。各コアコントロールには、複数のコントロール実装 (L6) と複数の証拠ソース (L7) を含めることができます。

要約すると、AWS コントロールカタログオントロジーには 7 つのレイヤーが含まれています。3 つは階層分類レイヤー (コントロールドメイン、コントロール目標、共通コントロール) です。もう 1 つのレイヤー (標準コントロール) では、規制または業界標準の要件について説明します。マッピングレイヤー (コアコントロール) は、特定のリソースタイプのコントロール結果を記述します。2 つのレイヤー (コントロール実装、コントロール証拠) は、特定のコントロール実装と証拠ソースを記述します。

このオントロジーは、コンプライアンス監査のために何百人もの顧客と連携した経験に基づいて、認定監査人の AWS チームによって設計されました。コントロールドメイン、コントロール目標、共通コントロール、標準コントロール (L1~L4) の概念は、業界全体で使用されています。これらは、一般的な業界パターンと NIST の推奨事項と一致します。残りの 3 つのレイヤー (L5-L7) は、リソースタイプやマネージドコントロールなどの既存の AWS 概念に基づいて設計されました。

Control Catalog へのアクセス

Control Catalog は、コンソールと Control Catalog アプリケーションプログラミングインターフェイス (API) を通じて使用できます。この API は、AWS 顧客として利用可能な一般的なコントロールと関連するメタデータを特定してフィルタリングするプログラムによる方法を提供します。詳細については、「[Control Catalog API Reference](#)」を参照してください。

Control Catalog のセキュリティ

でのクラウドセキュリティが最優先事項 AWS です。お客様は AWS、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からメリットを得られます。

セキュリティは、AWS とお客様の間の責任共有です。[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 のサービス で実行されるインフラストラクチャを保護する責任を担います AWS クラウド。は、お客様が安全に使用できるサービス AWS も提供します。サードパーティーの監査者は、[AWS コンプライアンスプログラム](#)コンプライアンスプログラムの一環として、当社のセキュリティの有効性を定期的にテストおよび検証。Control Catalog に適用され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AWS プログラムによる対象範囲内のサービスコンプライアンス](#)」を参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する によって決まり AWS のサービス ます。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、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、Control Catalog を使用する際の責任共有モデルの適用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 Control Catalog を設定する方法を示します。また、Control Catalog; リソースのモニタリングと保護 AWS のサービス に役立つ他の の使用方法についても説明します。

トピック

- [Control Catalog でのデータ保護](#)
- [Control Catalog の Identity and Access Management](#)
- [Control Catalog のコンプライアンス検証](#)
- [Control Catalog の耐障害性](#)
- [Control Catalog のインフラストラクチャセキュリティ](#)

Control Catalog でのデータ保護

責任 AWS [共有モデル](#)、AWS Control Catalog 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 はすべての 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責任が

あります AWS クラウド。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。

データ保護の目的で、認証情報を保護し AWS アカウント、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設定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。
- API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。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 暗号化ソリューションと、内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- 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 AWS を介して にアクセスするときに 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、または SDK を使用して AWS Control Catalog AWS CLI または他の AWS のサービスを使用する場合も同様です。AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、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。

データ暗号化

AWS Control Catalog は顧客データを保存しません。

保管中の暗号化

AWS Control Catalog は顧客データを暗号化しません。AWS Control Catalog によって保持または保持される顧客データがないため、保管時の暗号化に関する特定のガイドラインはありません。

転送中の暗号化

AWS Control Catalog は顧客データを暗号化しません。AWS Control Catalog によって機密データが交換または保持されないため、転送中の暗号化に関する特定のガイドラインはありません。

キー管理

暗号化キー管理は AWS Control Catalog には適用されません。

ネットワーク間トラフィックのプライバシー

ネットワーク間トラフィックのプライバシーは、AWS Control Catalog には適用されません。

Control Catalog の Identity and Access Management

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 AWS のサービス するのに役立つです。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS Control Catalog リソースの使用を許可する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

トピック

- [オーディエンス](#)
- [アイデンティティを使用した認証](#)
- [ポリシーを使用したアクセスの管理](#)
- [Control Catalog と IAM の連携方法](#)
- [Control Catalog のアイデンティティベースのポリシーの例](#)
- [Control Catalog のアイデンティティとアクセスのトラブルシューティング](#)

オーディエンス

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 (「[Control Catalog のアイデンティティ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 (「[Control Catalog 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 (「[Control Catalog のアイデンティティベースのポリシーの例](#)」を参照)

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。、IAM ユーザー AWS アカウントのルートユーザー、または IAM ロールを引き受けることで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 Identity Center)、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 ID 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、 は SDK と CLI AWS を提供してリクエストを暗号化して署名します。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 ルートユーザー

を作成するときは AWS アカウント、まず、すべての AWS のサービス および リソースへの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 つのサインインアイデンティティから始めます。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として、人間のユーザーが一時的な認証情報 AWS のサービス を使用して 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を使用する必要があります。

フェデレーテッド ID 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、または ID Directory Service ソースの認証情報 AWS のサービス を使用して 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。詳細については、IAM ユーザーガイドの「[ID プロバイダーとのフェデレーションを使用してアクセスすることを人間のユーザーに要求する AWS](#)」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 \(コンソール\)](#) に切り替えるか、または [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。AWS CLI AWS 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の管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは、アイデンティティまたはリソースに関連付けられたときにアクセス許可を定義します。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 AWS を評価します。ほとんどのポリシーは JSON ドキュメント AWS としてに保存されます。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は、IAM の AWS マネージドポリシーを使用できません。

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によって付与されるアクセス許可の最大数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。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「[ポリシー評価ロジック](#)」を参照してください。

Control Catalog と IAM の連携方法

IAM を使用して AWS Control Catalog へのアクセスを管理する前に、AWS Control Catalog で使用できる IAM 機能を確認してください。

Control Catalog で使用できる IAM 機能

IAM 機能	AWS Control Catalog 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	あり
ポリシー条件キー	あり
ACL	なし
ABAC (ポリシー内のタグ)	いいえ
一時的な認証情報	あり

IAM 機能	AWS Control Catalog のサポート
プリンシパル権限	いいえ
サービスロール	いいえ
サービスリンクロール	いいえ

AWS Control Catalog およびその他の 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については、IAM ユーザーガイドの[AWS 「IAM と連携する のサービス」](#)を参照してください。

AWS Control Catalog の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のサポート: あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。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。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の[「IAM JSON ポリシーの要素のリファレンス」](#)を参照してください。

AWS Control Catalog のアイデンティティベースのポリシーの例

AWS Control Catalog のアイデンティティベースのポリシーの例を表示するには、「」を参照してください[Control Catalog のアイデンティティベースのポリシーの例](#)。

AWS Control Catalog 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、フェデレーテッドユーザー、またはを含めることができます AWS のサービス。

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 Control Catalog 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 JSON AWS ポリシーを使用して、誰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。

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 Control Catalog 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 Control Catalog で定義されるアクション](#)」を参照してください。

AWS Control Catalog 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。

```
controlcatalog
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [  
  "controlcatalog:ListCommonControls",  
  "controlcatalog:ListDomains"  
]
```

ワイルドカード *を使用して複数のアクションを指定することができます。例えば、List という単語で始まるすべてのアクションを指定するには、次のアクションを含めます。

```
"Action": "controlcatalog:List*"
```

AWS Control Catalog のアイデンティティベースのポリシーの例を表示するには、「」を参照してください [Control Catalog のアイデンティティベースのポリシーの例](#)。

AWS Control Catalog のポリシーリソース

ポリシーリソースのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰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。リソースレベルのアクセス許可をサポートしないアクションの場合は、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すために、ワイルドカード (*) を使用します。

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

AWS Control Catalog リソースタイプとその ARNs [「AWS Control Catalog で定義されるリソース」](#) を参照してください。各リソースの ARN を指定できるアクションについては、[「AWS Control Catalog で定義されるアクション」](#) を参照してください。

AWS Control Catalog ドメインの Amazon リソースネーム (ARN) 形式は次のとおりです。

```
arn:${Partition}:controlcatalog:::domain/${domainId}
```

AWS Control Catalog の目標の ARN 形式は次のとおりです。

```
arn:${Partition}:controlcatalog:::objective/${objectiveId}
```

AWS Control Catalog の共通コントロールには、次の ARN 形式があります。

```
arn:${Partition}:controlcatalog:::commonControl/${commonControlId}
```

ARN の形式の詳細については、[「Amazon リソースネーム \(ARN\)」](#) を参照してください。

たとえば、ステートメントで*i-1234567890abcdef0*ドメインを指定するには、次の ARN を使用します。

```
"Resource": "arn:aws:controlcatalog:::domain/i-1234567890abcdef0"
```

特定のアカウントに属するすべてのインスタンスを指定するには、ワイルドカード ***を使用します。

```
"Resource": "arn:aws:controlcatalog:::domain/*"
```

リソースを作成するためのアクションなど、一部の AWS Control Catalog 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": "*"
```

一部の AWS Control Catalog API アクションは、複数のリソースをサポートしています。たとえば、は共通のコントロール、目標、ドメイン `ListCommonControls` にアクセスするため、プリンシパルにはこれらの各リソースにアクセスするためのアクセス許可が必要です。複数リソースを単一ステートメントで指定するには、ARN をカンマで区切ります。

```
"Resource": [  
    "commonControl",  
    "objective",  
    "domain"
```

AWS Control Catalog のアイデンティティベースのポリシーの例を表示するには、「」を参照してください [Control Catalog のアイデンティティベースのポリシーの例](#)。

AWS Control Catalog 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 JSON AWS ポリシーを使用して、誰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。

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 Control Catalog の条件キー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 Control Catalog の条件キー](#)」を参照してください。条件キーを使用できるアクションとリソースについては、「[AWS Control Catalog で定義されるアクション](#)」を参照してください。

AWS Control Catalog のアイデンティティベースのポリシーの例を表示するには、「[アイデンティティベースのポリシーの例](#)」を参照してください。

AWS Control Catalog ACLs

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 Control Catalog での ABAC

ABAC (ポリシー内のタグ) のサポート: なし

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 リソースにタグをアタッチし、プリンシパルのタグがリソースのタグと一致するときにオペレーションを許可するように 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 Control Catalog 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、フェデレーションまたはスィッチロールの使用時に自動的に作成されます。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 AWS を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 Control Catalog のクロスサービスプリンシパルアクセス許可

転送アクセスセッション (FAS) のサポート: なし

転送アクセスセッション (FAS) は、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウストリームサービス AWS のサービス へのリクエストをリクエストする を使用します。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 Control Catalog 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。

Warning

サービスロールのアクセス許可を変更すると、AWS Control Catalog の機能が破損する可能性があります。AWS Control Catalog が指示する場合にのみ、サービスロールを編集します。

AWS Control Catalog 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、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント、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。

Control Catalog のアイデンティティベースのポリシーの例

デフォルトでは、ユーザーとロールには AWS Control Catalog 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。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。

これらのサンプルの JSON ポリシードキュメントを使用して 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「[IAM ポリシーを作成する \(コンソール\)](#)」を参照してください。

各リソースタイプの ARNs [「AWS Control Catalog のアクション、リソース、および条件キー」](#)を参照してください。

トピック

- [ポリシーに関するベストプラクティス](#)
- [ユーザーが自分の権限を表示できるようにする](#)
- [ユーザーに AWS Control Catalog からのリソースの表示を許可する](#)

ポリシーに関するベストプラクティス

ID ベースのポリシーは、アカウント内で誰かが AWS Control Catalog リソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションでは、AWS アカウントに費用が発生する場合があります。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 管理ポリシーを開始し、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に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にアクセス許可を付与する AWS 管理ポリシーを使用します。これらはで使用できます AWS アカウント。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することで、アクセス許可をさらに減らす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。条件を使用して、サービスアクションがなどの特定の を通じて使用されている場合に AWS のサービス、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 CloudFormation。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 - IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、MFA をオンにしてセキュリティを強化します。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 でのセキュリティベストプラクティス](#)」を参照してください。

ユーザーが自分の権限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 または AWS API を使用してプログラムでこのアクションを実行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:ListGroupsWithUser",

```

```

        "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": "*"
}
]
}

```

ユーザーに AWS Control Catalog からのリソースの表示を許可する

次のポリシーは、AWS Control Catalog からドメイン、目的、一般的なコントロールを一覧表示するアクセス許可を付与します。

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ManageControlCatalogAccess",
      "Effect": "Allow",
      "Action": [
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives",
        "controlcatalog:ListCommonControls"
      ],
    },
  ],
}

```

```
    "Resource": "*"
  }
]
}
```

Control Catalog のアイデンティティとアクセスのトラブルシューティング

次の情報は、AWS Control Catalog と IAM の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちます。

トピック

- [Control Catalog でアクションを実行する権限がありません](#)
- [iam:PassRole を実行する権限がありません](#)
- [Control Catalog リソース AWS アカウント へのアクセス権を自分の外部のユーザーに付与したい](#)

Control Catalog でアクションを実行する権限がありません

アクションを実行する権限がないというエラーが表示された場合は、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要な `controlcatalog:GetWidget` アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
controlcatalog:GetWidget on resource: my-example-widget
```

この場合、`controlcatalog:GetWidget` アクションを使用して *my-example-widget* リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がありません

`iam:PassRole` アクションを実行する権限がないというエラーが表示された場合は、AWS Control Catalog にロールを渡すことができるようにポリシーを更新する必要があります。

一部の AWS のサービスでは、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡すアクセス許可が必要です。

次の例のエラーは、という IAM ユーザーがコンソールを使用して marymajor AWS Control Catalog でアクションを実行しようとするると発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与されたアクセス許可が必要です。Mary には、ロールをサービスに渡すアクセス許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

Control Catalog リソース AWS アカウント へのアクセス権を自分の外部のユーザーに付与したい

他のアカウントのユーザーや組織外の人、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- AWS Control Catalog がこれらの機能をサポートしているかどうかを確認するには、「」を参照してください [Control Catalog と IAM の連携方法](#)。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの [「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」](#) を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの [「サードパーティー AWS アカウント が所有する へのアクセスを提供する」](#) を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの [外部で認証されたユーザー \(ID フェデレーション\) へのアクセスの許可](#) を参照してください。

- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、IAM ユーザーガイドの [IAM でのクロスアカウントのリソースへのアクセス](#) を参照してください。

Control Catalog 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AWS のサービス プログラムによる対象範囲内](#)」の「コンプライアンス」を参照し、関心のあるコンプライアンスプログラムを選択します。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。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「[Downloading Reports in AWS Artifact](#)」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービスは、お客様のデータの機密性、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まります。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 のサービス、[AWS 「セキュリティドキュメント」](#)を参照してください。

Control Catalog 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ゾーンを中心に構築されています。は、低レイテンシー、高スループット、高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティゾーン AWS リージョン を提供します。アベイラビリティゾーンでは、ゾーン間で中断することなく自動的にフェー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よりも可用性、フォールトトレランス、および拡張性が優れています。

AWS リージョン およびアベイラビリティ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。

Control Catalog 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 Control Catalog は、ホワイトペーパー「[Amazon Web Services: セキュリティプロセスの概要](#)」に記載されている AWS グローバルネットワークセキュリティ手順で保護されています。

AWS 公開された API コールを使用して、ネットワーク経由で Control Catalog にアクセスします。クライアントで Transport Layer Security (TLS) 1.0 以降がサポートされている必要があります。TLS 1.2 以降が推奨されています。また、DHE (Ephemeral Diffie-Hellman) や ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。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。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、[AWS Security Token Service](#) (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

Control Catalog の設定と脆弱性の分析

設定と IT コントロールは、AWS とお客様の間の責任共有です。詳細については、AWS [「責任共有モデル」](#) を参照してください。

AWS Control Catalog のモニタリング

モニタリングは、AWS Control Catalog およびその他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。には、AWS Control Catalog をモニタリングし、問題が発生したときに報告し、必要に応じて自動アクションを実行するための以下のモニタリングツール AWS が用意されています。

- AWS CloudTrail は、AWS アカウントによって、またはアカウントに代わって行われた API コールおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。呼び出し元のユーザーとアカウント AWS、呼び出し元の送信元 IP アドレス、呼び出しの発生日時を特定できます。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。

を使用した Control Catalog API コールのログ記録 AWS CloudTrail

AWS Control Tower Control Catalog の一部として、ユーザー AWS CloudTrail、ロール、またはサービスによって実行されたアクションを記録する AWS サービスがと統合されています。CloudTrail は、Control Catalog 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。キャプチャされた呼び出しには、コントロールを有効または無効にするなどの AWS Control Tower コンソールから直接の呼び出しや、Control Catalog API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、コントロールカタログのコントロールに関連するイベントなど、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 で収集された情報を使用して、Control Catalog に対するリクエスト (による AWS Control Tower)、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

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 のコントロールカタログ情報

CloudTrail は、アカウントの作成 AWS アカウント 時に で有効になります。Control Catalog でアクティビティが発生すると、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。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。

Control Catalog 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ついては、証跡を作成します。証跡により、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 パーティション内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 ログで収集されたイベントデータをさらに分析して処理 AWS のサービス するように他の を設定できます。詳細については、次を参照してください:

- [追跡を作成するための概要](#)
- [CloudTrail がサポートされているサービスと統合](#)
- 「[CloudTrail の Amazon SNS 通知の設定](#)」
- [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 Control Catalog アクションは CloudTrail によってログに記録され、[Control Catalog API リファレンスに記載されています](#)。たとえば、ListCommonControls、ListObjectives、ListDomains 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。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか。
- 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 エlement](#)」を参照してください。

Control Catalog ログファイルエントリについて

「トレイル」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、任意の出典からの単一のリクエストを表し、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に関する情報が含まれます。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、ListDomains アクションを示す CloudTrail ログエントリです。

```
{
  eventVersion:"1.05",
  userIdentity:{
    type:"IAMUser",
    principalId:"principalId",
    arn:"arn:aws:iam::accountId:user/userName",
    accountId:"111122223333",
    accessKeyId:"accessKeyId",
    userName:"userName",
    sessionContext:{
      sessionIssuer:{
      },
      webIdFederationData:{
      },
      attributes:{
        mfaAuthenticated:"false",
        creationDate:"2020-11-19T07:32:06Z"
      }
    }
  },
  eventTime:"2020-11-19T07:32:36Z",
  eventSource:"controlcatalog.amazonaws.com",
  eventName:"ListDomains",
  awsRegion:"us-west-2",
  sourceIPAddress:"sourceIPAddress",
  userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  requestParameters: null,
  responseElements: null,
  requestId:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
  eventId:"a782029a-959e-4549-81df-9f6596775cb0",
  readOnly:false,
  eventType:"AwsApiCall",
  recipientAccountId:"recipientAccountId"
}
```

インターフェイスエンドポイント (AWS PrivateLink) を使用して Control Catalog にアクセスする

を使用して AWS PrivateLink、VPC と Control Catalog の間にプライベート接続を作成できます。インターネットゲートウェイ、NAT デバイス、VPN 接続、または Direct Connect 接続を使用せずに、VPC 内にあるかのように AWS Control Catalog にアクセスできます。VPC 内のインスタンスは、Control Catalog にアクセスするためにパブリック IP アドレスを必要としません。

このプライベート接続を確立するには、AWS PrivateLink を利用したインターフェイスエンドポイントを作成します。インターフェイスエンドポイントに対して有効にする各サブネットにエンドポイントネットワークインターフェイスを作成します。これらは、Control Catalog 宛てのトラフィックのエントリーポイントとして機能するリクエスト管理のネットワークインターフェイスです。

詳細については、「AWS PrivateLink ガイド」の [「Access AWS のサービス through AWS PrivateLink」](#) を参照してください。

AWS Control Catalog に関する考慮事項

Control Catalog のインターフェイスエンドポイントを設定する前に、「AWS PrivateLink ガイド」の [「考慮事項」](#) を参照してください。

Control Catalog は、インターフェイスエンドポイントを介したすべての API アクションの呼び出しをサポートしています。

Control Catalog のインターフェイスエンドポイントを作成する

Control Catalog のインターフェイスエンドポイントは、Amazon VPC コンソールまたは AWS Command Line Interface () を使用して作成できます AWS CLI。詳細については、「AWS PrivateLink ガイド」の [「インターフェイスエンドポイントを作成」](#) を参照してください。

次のサービス名を使用して Control Catalog のインターフェイスエンドポイントを作成します。

```
com.amazonaws.region.controlcatalog
```

インターフェイスエンドポイントのプライベート DNS を有効にすると、デフォルトのリージョン DNS 名を使用して Control Catalog に API リクエストを行うことができます。例えば、`service-name.us-east-1.amazonaws.com`。

インターフェイスエンドポイントのエンドポイントポリシーを作成する

エンドポイントポリシーは、インターフェイスエンドポイントにアタッチできる IAM リソースです。デフォルトのエンドポイントポリシーでは、インターフェイスエンドポイントを介して Control Catalog へのフルアクセスを許可します。VPC から Control Catalog に許可されるアクセスを制御するには、カスタムエンドポイントポリシーをインターフェイスエンドポイントにアタッチします。

エンドポイントポリシーは以下の情報を指定します。

- アクションを実行できるプリンシパル (AWS アカウント、IAM ユーザー、IAM ロール)。
- 実行可能なアクション。
- このアクションを実行できるリソース。

詳細については、AWS PrivateLink ガイドの[Control access to services using endpoint policies \(エンドポイントポリシーを使用してサービスへのアクセスをコントロールする\)](#)を参照してください。

例: Control Catalog アクションの VPC エンドポイントポリシー

以下は、カスタムエンドポイントポリシーの例です。このポリシーをインターフェイスエンドポイントにアタッチすると、すべてのリソースのすべてのプリンシパルに対して、リストされている AWS Control Catalog アクションへのアクセスが許可されます。

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives",
        "controlcatalog:ListCommonControls"
      ],
      "Resource": "*"
    }
  ]
}
```

Note

GetControl および ListControls API オペレーションには、デフォルトのフルアクセス許可である別のアクセス許可が必要です。例については、[「デフォルトのエンドポイントポリシー」](#)を参照してください。

Control Catalog セキュリティ情報ガイドのドキュメント履歴

次の表に、Control Catalog のドキュメントリリースを示します。

変更	説明	日付
初回リリース	Control Catalog APIsとセキュリティ情報ガイドの初回リリース。	2024 年 4 月 8 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。