aws

管理ガイド

Amazon Chime SDK

Amazon Chime SDK: 管理ガイド

Table of Contents

Amazon Chime SDK とは

Amazon Chime SDK は、デベロッパーがウェブアプリケーションまたはモバイルアプリケーションにメッセージング、オーディオ、ビデオ、および画面共有機能を追加するために使用できるリアルタイム通信コンポーネントのセットを提供します。例えば、デベロッパーはヘルスアプリケーションに動画を追加し、患者の健康問題をリモートで調査したり、公衆交換電話網 (PSTN) との統合用にカスタマイズされた音声プロンプトを作成したりできます。Amazon Chime SDK を使用することで、デベロッパーは、コスト、複雑さ、および独自のリアルタイム通信インフラストラクチャとサービスの作成と維持に伴う摩擦を排除できます。

詳細については、AWS「Amazon Chime SDK」ページを参照してください。

料金

Amazon Chime SDK は、前払い料金なしで pay-for-use 料金を提供します。SDK を実装するデベロッパーは、使用可能なメディアモダリティ (オーディオ、ビデオ、スクリーン共有) の一部またはすべてを 1 つのレートで実装することを選択できます。メッセージング、メディアパイプライン、音声エンハンスメント、PSTN オーディオ機能も pay-for-use 料金で利用できます。詳細については、「Amazon Chime SDK の料金」を参照してください。

前提条件

Amazon Chime SDK コンソールAWSにアクセスして Amazon Chime 管理者アカウントを作成するには、 アカウントが必要です。

Amazon Web Services アカウントの作成

Amazon Chime SDK の管理者アカウントを作成する前に、まずAWSアカウントを作成する必要があります。

トピック

- AWS アカウントへのサインアップ
- 管理ユーザーの作成

AWS アカウントへのサインアップ

AWS アカウントがない場合は、以下のステップを実行して作成します。

AWS アカウント にサインアップするには

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話のキーパッドを使用して検証コードを入力するように求められます。

   AWS アカウントにサインアップすると、AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービスとリソースへのアクセス権があります。セキュリティのベストプラクティスとして、管理ユーザーに管理アクセスを割り当て、ルートユーザーアクセスが必要なタスクを実行する場合にのみ、ルートユーザーを使用してください。

サインアップ処理が完了すると、AWS からユーザーに確認メールが送信されます。https://aws.amazon.com/ の [アカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理ユーザーの作成

AWS アカウント にサインアップしたら、AWS アカウントのルートユーザー をセキュリティで保護し、AWS IAM Identity Center を有効にして、管理ユーザーを作成します。これにより、日常的なタスクにルートユーザーを使用しないようにします。

AWS アカウントのルートユーザーをセキュリティで保護する

1. [ルートユーザー] を選択し、AWS アカウント のメールアドレスを入力して、アカウント所有者として AWS Management Console にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、「AWS サインイン User Guide」の「Signing in as the root user」を参照してください。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、「IAM ユーザーガイド」の「AWS アカウント のルートユーザーの仮想 MFA デバイスを有効にする (コンソール)」を参照してください。

管理ユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Center の有効化」を参照してください。
2. IAM アイデンティティセンターで、管理ユーザーに管理者アクセスを付与します。

   IAM アイデンティティセンターディレクトリ をアイデンティティソースとして使用するチュートリアルについては、「AWS IAM Identity Center ユーザーガイド」の「デフォルトの IAM アイデンティティセンターディレクトリ でユーザーアクセスを設定する」を参照してください。

管理ユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM アイデンティティセンターのユーザーを使用してサインインする方法については、「AWS サインイン User Guide」の「Signing in to the AWS access portal」を参照してください。

Amazon Chime SDK のセキュリティ

AWS ではクラウドセキュリティが最優先事項です。セキュリティを最も重視する組織の要件を満たすために構築された AWS のデータセンターとネットワークアーキテクチャは、お客様に大きく貢献します。

セキュリティは、AWS とお客様とが共有する責務です。責任共有モデルではこれを、クラウドのセキュリティ、およびクラウド内で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 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負います。また AWS は、安全に使用できるサービスを提供します。AWS コンプライアンスプログラムの一環として、サードパーティー監査者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ます。Amazon Chime SDK 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 AWS 対象範囲内のサービスコンプライアンスプログラム」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 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、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、Amazon Chime SDK 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 Amazon Chime SDK を設定する方法を示します。また、Amazon Chime SDK リソースのモニタリングや保護に役立つ他の AWSのサービスの使用方法についても説明します。

トピック

- Amazon Chime SDK のサービスにリンクされたロールの使用
- Amazon Chime SDK でのログ記録とモニタリング
- Amazon Chime SDK のコンプライアンス検証
- Amazon Chime SDK の耐障害性
- Amazon Chime SDK のインフラストラクチャセキュリティ

Amazon Chime SDK 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 Amazon Chime SDK リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は、追加費用なしで使用できる AWS のサービスです。

トピック

- 対象者
- アイデンティティによる認証
- ポリシーを使用したアクセス権の管理

対象者

AWS Identity and Access Management (IAM) の使用方法は、Amazon Chime SDK で行う作業によって異なります。

サービスユーザー – ジョブを実行するために Amazon Chime SDK サービスを使用する場合は、管理者から必要なアクセス許可と認証情報が与えられます。さらに多くの Amazon Chime SDK 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。Amazon Chime SDK の機能にアクセスできない場合は、「」を参照してくださいAmazon Chime SDK 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。

サービス管理者 – 社内の Amazon Chime SDK リソースを担当している場合は、通常、Amazon Chime SDK へのフルアクセスがあります。従業員がどの Amazon Chime SDK 機能やリソースにアクセスする必要があるかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。Amazon Chime SDK で IAM を利用する方法の詳細については、「」を参照してくださいAmazon Chime SDK と IAM の連携方法。

IAM 管理者 – IAM 管理者は、Amazon Chime SDK へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる Amazon Chime SDK 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Amazon Chime SDK アイデンティティベースのポリシーの例。

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、AWS アカウントのルートユーザーもしくは IAM 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、認証を受ける (AWS にサインインする) 必要があります。

ID ソースから提供された認証情報を使用して、フェデレーティッドアイデンティティとして AWS にサインインできます。 AWS IAM Identity Centerフェデレーティッドアイデンティティの例としては、(IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報などがあります。フェデレーティッドアイデンティティとしてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーションを使用して AWSにアクセスする場合、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、AWS Management Console または AWS アクセスポータルにサインインできます。AWS への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。

プログラムで AWS にアクセスする場合、AWS は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) を提供し、認証情報でリクエストに暗号で署名します。AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。リクエストに署名する推奨方法の使用については、『IAM ユーザーガイド』の「AWS API リクエストの署名」を参照してください。

使用する認証方法を問わず、追加のセキュリティ情報の提供が求められる場合もあります。例えば、AWS では、アカウントのセキュリティ強化のために多要素認証 (MFA) の使用をお勧めしています。詳細については、「AWS IAM Identity Center ユーザーガイド」の「Multi-factor authentication (多要素認証)」 および「IAM ユーザーガイド」の「AWS での多要素認証 (MFA) の使用」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場合は、そのアカウントのすべての AWS のサービスとリソースに対して完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。このアイデンティティは AWS アカウントのルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることによってアクセスできます。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。ルートユーザーの認証情報は保護し、ルートユーザーで

しか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、『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。

IAM ユーザーとグループ

IAM ユーザーは、1 人のユーザーまたは 1 つのアプリケーションに対して特定の権限を持つ AWS アカウント 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーション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「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する権限を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、特定の権限を持つ、AWS アカウント 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。ロールを切り替えることによって、AWS Management Console で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、AWS CLI または AWS API オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

一時的な認証情報を持った IAM ロールは、以下の状況で役立ちます。

- フェデレーションユーザーユーザーアクセス – フェデレーションアイデンティティに権限を割り当てるには、ロールを作成してそのロールの権限を定義します。フェデレーティッドアイデンティティが認証されると、そのアイデンティティはロールに関連付けられ、ロールで定義されている

権限が付与されます。フェデレーションの詳細については、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー向けロールの作成」を参照してください。IAM アイデンティティセンターを使用する場合、権限セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。権限セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「権限セット」を参照してください。

- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の AWS のサービスでは、(ロールをプロキシとして使用する代わりに) リソースにポリシーを直接アタッチできます。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違いについては、「IAM ユーザーガイド」の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。
- クロスサービスアクセス - 一部の AWS のサービスでは、他の AWS のサービスの機能を使用します。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの権限、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して AWS でアクションを実行するユーザーは、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、AWS のサービスを呼び出すプリンシパルの権限を、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 リクエストは、サービスが、完了するために他の AWS のサービス またはリソースとのやりとりを必要とするリクエストを受け取ったときにのみ行われます。この場合、両方のアクションを実行するための許可が必要です。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。
  - サービスロール - 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 に権限を委任するロールの作成」を参照してください。
  - サービスリンクロール - サービスリンクロールは、AWS のサービス にリンクされた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。サービスリンクロールは、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、サービスリンクロールの権限を表示できますが、編集することはできません。

- Amazon EC2 で実行されているアプリケーション - EC2 インスタンスで実行され、AWS CLI または AWS API 要求を行っているアプリケーションの一時的な認証情報を管理するには、IAM ロールを使用できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスに添付されたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用してアクセス許可を付与する」を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、「IAM ユーザーガイド」の「(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?」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 でアクセス権を管理するには、ポリシーを作成して AWS アイデンティティまたはリソースにアタッチします。ポリシーは AWS のオブジェクトであり、アイデンティティやリソースに関連付けて、これらの権限を定義します。AWS は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うと、これらのポリシーを評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。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構造と内容の詳細については、「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 AWSJSON 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。

デフォルトでは、ユーザーやロールに権限はありません。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。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの権限を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。このポリシーがあるユーザーは、AWS Management Console、AWS CLI、または AWS API からロール情報を取得できます。

アイデンティティベースポリシー

アイデンティティベースポリシーは、IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 権限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、および条件を制御します。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 ポリシーの作成」を参照してください。

アイデンティティベースポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれます。管理ポリシーは、AWS アカウント 内の複数のユーザー、グループ、およびロールにアタッチできるスタンドアロンポリシーです。マネージドポリシーには、AWS マネージドポリシーとカスタマー管理ポリシーがあります。マネージドポリシーまたは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「マネージドポリシーとインラインポリシーの比較」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。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制御できます。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は、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。

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は使用できません。

AWS Amazon Chime SDK の マネージドポリシー

ユーザー、グループ、ロールにアクセス許可を追加するには、自分でポリシーを作成するよりも、AWS 管理ポリシーを使用する方が簡単です。チームに必要な権限のみを提供する IAM カスタマーマネージドポリシーを作成するには、時間と専門知識が必要です。すぐに使用を開始するために、AWS マネージドポリシーを使用できます。これらのポリシーは、一般的なユースケースを対象範囲に含めており、AWS アカウントで利用できます。AWS マネージドポリシーの詳細については、「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 のサービスは、AWS マネージドポリシーを維持および更新します。AWS マネージドポリシーの許可を変更することはできません。サービスでは、新しい機能を利用できるようにするために、AWS マネージドポリシーに権限が追加されることがあります。この種類の更新は、ポリシーがアタッチされている、すべてのアイデンティティ (ユーザー、グループおよびロール) に影響を与えます。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスが 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。サービスは、AWS マネージドポリシーから権限を削除しないため、ポリシーの更新によって既存の権限が破棄されることはありません。

さらに、AWS では、複数のサービスにまたがるジョブ機能のためのマネージドポリシーもサポートしています。例えば、ReadOnlyAccess AWS マネージドポリシーでは、すべての AWS のサービスおよびリソースへの読み取り専用アクセスを許可します。あるサービスで新しい機能を立ち上げる場合は、AWS は、追加された演算とリソースに対し、読み込み専用の権限を追加します。ジョブ機能ポリシーのリストと説明については、IAM ユーザーガイドの「AWS ジョブ機能のマネージドポリシー」を参照してください。

アクセスコントロールリスト (ACL)

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権限を持つかをコントロールします。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。

Simple Storage Service (Amazon S3)、AWS WAF、および Amazon VPC は、ACL をサポートするサービスの例です。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS では、他の一般的ではないポリシータイプをサポートしています。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- 権限の境界 - 権限の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる許可の上限を設定する高度な機能です。エンティティに権限の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとその権限の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、権限の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。権限の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティの権限の境界」を参照してください。

- サービスコントロールポリシー (SCP) - SCP は、AWS Organizations で組織や組織単位 (OU) の最大権限を指定する JSON ポリシーです。AWS Organizations は、顧客のビジネスが所有する複数の AWS アカウント をグループ化し、一元的に管理するサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP はメンバーアカウントのエンティティに対する権限を制限します (各 AWS アカウントのルートユーザー など)。Organizations と SCP の詳細については、『AWS Organizations ユーザーガイド』の「SCP の仕組み」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限の範囲は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。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」をご参照ください。

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権限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「Policy evaluation logic (ポリシーの評価ロジック)を参照してください。

Amazon Chime SDK と IAM の連携方法

IAM を使用して Amazon Chime SDK へのアクセスを管理する前に、Amazon Chime SDK で使用できる IAM 機能について学びます。Amazon Chime SDK およびその他の AWSのサービスが IAM 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AWS「IAM と連携する のサービス」を参照してください。

トピック

- Amazon Chime SDK アイデンティティベースのポリシー
- リソース
- 例

Amazon Chime SDK アイデンティティベースのポリシー

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、アクションを許可または拒否する条件を指定できます。Amazon Chime SDK は、特定のアクション、リソース、および条件キーをサポートしています。JSON ポリシーで使用するすべての要素については、「IAM ユーザーガイド」の「IAM JSON ポリシーエレメントのリファレンス」を参照してください。

アクション

管理者は AWS JSON 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。

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。ポリシーアクションの名前は通常、関連する AWS API オペレーションと同じです。一致する API オペレーションのない権限のみのアクションなど、いくつかの例外があります。また、ポリシーに複数アクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

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権限を付与するポリシーで使用されます。

アクションの詳細については、「サービス認証リファレンス」の「Amazon Chime 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。

条件キー

Amazon Chime SDK は、サービス固有の条件キーのセットを提供します。詳細については、「サービス認証リファレンス」の「Amazon Chime の条件キー」を参照してください。

リソース

Amazon Chime SDK では、ポリシーでのリソース ARNs の指定がサポートされています。詳細については、「Amazon Chime で定義されるリソースタイプ」を参照してください。

例

Amazon Chime SDK 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Amazon Chime SDK アイデンティティベースのポリシーの例。

音声分析での暗号化の使用

Amazon Chime SDK 音声分析は、音声埋め込みの生成に使用される音声ファイルを保存します。ファイルは、ユーザーが作成、所有、管理する対称カスタマーマネージドキーを使用して暗号化されます。この暗号化レイヤーを完全に制御できるため、次のようなタスクを実行できます。

- キーポリシーの策定と維持
- IAM ポリシーとグラントの策定と維持
- キーポリシーの有効化と無効化
- 暗号化素材のローテーション
- タグの追加
- キーエイリアスの作成
- キー削除のスケジュール設定

詳細については、AWS Key Management Service デベロッパーガイドの「カスタマーマネージドキー」を参照してください。

保管時の暗号化について

音声分析では、保管中のすべてのユーザーデータが暗号化されます。新しい音声プロファイルドメインを作成するときは、サービスが保管中のデータを暗号化するために使用する対称カスタマーマネージドキーを提供する必要があります。キーを所有、管理、制御します。

キーは、音声埋め込みにスピーカーを登録するために使用される音声ファイルのみを暗号化します。

音声分析は、許可を作成してキーにアクセスします。許可の詳細については、次のセクションを参照してください。

音声分析で許可を使用する方法を理解する

音声分析では、カスタマーマネージドキーを使用するには許可が必要です。音声プロファイルドメインを作成すると、関連付けられた Amazon Chime SDK Voice Connector は、KMS AWS に`CreateGrant`リクエストを送信することで、ユーザーに代わって許可を作成します。この権限は、以下の内部オペレーションでキーを使用するために必要です。

- 指定された対称カスタマーマネージドキー ID AWS が有効であることを確認するために、KMS に`DescribeKey`リクエストを送信します。

- KMS キーにGenerateDataKeyリクエストを送信して、オブジェクトを暗号化するデータキーを作成します。
- Decrypt AWS リクエストを KMS に送信して、暗号化されたデータキーを復号し、データの暗号化に使用できるようにします。
- KMS AWS にRetireGrantリクエストを送信して、音声プロファイルドメインに使用される許可を廃止します。
- サーバー側の暗号化を使用して Amazon S3 にファイルを保存する。

権限へのアクセスはいつでも取り消すことができ、サービスのキーへのアクセスはいつでも削除できます。これを行うと、音声分析はキーで暗号化されたデータにアクセスできなくなります。これは、そのデータに依存するすべてのオペレーションに影響し、スピーカー検索ワークフローでAccessDeniedException工ラーや障害が発生します。

音声分析のキーポリシー

キーポリシーは、カスタマーマネージドキーへのアクセスを制御します。すべてのカスタマーマネージドキーには、キーを使用できるユーザーとその使用方法を決定するポリシーステートメントを含む、厳密に 1 つのキーポリシーが必要です。キーを作成するときに、キーポリシーを指定できます。詳細については、AWS Key Management Service デベロッパーガイドの「キーポリシーの使用」を参照してください。

```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow key access to Amazon Chime SDK voice analytics.",
            "Effect": "Allow",
            "Principal": {
                "AWS": "your_user_or_role_ARN"
            },
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "kms:ViaService": [
                        "chimevoiceconnector.region.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

ポリシーでアクセス許可を指定する方法については、AWS Key Management Service 開発者ガイドの「IAM ポリシーステートメントでの KMS キーの指定」を参照してください。

キーアクセスのトラブルシューティングについては、AWS Key Management Service デベロッパーガイドの「キーアクセスのトラブルシューティング」を参照してください。

暗号化コンテキストの使用

暗号化コンテキストは、データに関する追加のコンテキスト情報を含むキーと値のペアのオプションセットです。 AWSKMS は、暗号化コンテキストを使用して認証された暗号化をサポートします。

暗号化リクエストに暗号化コンテキストを含めると、KMS AWS は暗号化コンテキストを暗号化されたデータにバインドします。データを復号化するには、そのリクエストに (暗号化時と) 同じ暗号化コンテキストを含めます。

音声分析では、すべての AWS KMS 暗号化オペレーションで同じ暗号化コンテキストを使用します。ここで、キーは `aws:chime:voice-profile-domain:arn`で、値はリソースの Amazon リソースネーム (ARN) です。

次の例は、一般的な暗号化コンテキストを示しています。

```
"encryptionContext": {
    "aws:chime:voice-profile-domain:arn": "arn:aws:chime:us-west-2:111122223333:voice-profile-domain/sample-domain-id"
}
```

また、カスタマー管理キーがどのように使用されているかを特定するために、暗号化コンテキストを監査レコードおよびログで使用することもできます。暗号化コンテキストは、 CloudTrail または ログによって生成された CloudWatch ログにも表示されます。

暗号化コンテキストを使用してキーへのアクセスを制御する

対称カスタマーマネージドキー (CMK) へのアクセスを制御するための条件として、キーポリシーと IAM ポリシー内の暗号化コンテキストを使用することもできます。付与する際に、暗号化コンテキストの制約を使用することもできます。

音声分析では、権限の暗号化コンテキストの制約を使用して、アカウントまたはリージョンのカスタマーマネージドキーへのアクセスを制御します。権限の制約では、権限によって許可されるオペレーションで指定された暗号化コンテキストを使用する必要があります。

次のキーポリシーステートメントの例では、特定の暗号化コンテキストのカスタマーマネージドキーへのアクセスを許可します。ポリシーステートメントの条件では、許可に暗号化コンテキストを指定する暗号化コンテキストの制約が必要です。

```
{
    "Sid": "Enable DescribeKey",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
    },
    "Action": "kms:DescribeKey",
    "Resource": "*"
},
{
    "Sid": "Enable CreateGrant",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
    },
    "Action": "kms:CreateGrant",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:chime:voice-profile-domain:arn":
 "arn:aws:chime:us-west-2:111122223333:voice-profile-domain/sample-domain-id"
        }
    }
}
```

暗号化キーのモニタリング

Amazon Chime SDK Voice Connector は KMS AWS にリクエストを送信し、それらのリクエストは または CloudWatch ログで CloudTrail 追跡できます。

CreateGrant

カスタマーマネージドキーを使用して音声プロファイルドメインリソースを作成すると、関連付けられた Voice Connector は、ユーザーに代わってAWSアカウントの KMS キーにアクセスするCreateGrantリクエストを送信します。Voice Connector が作成する許可は、カスタマーマネージドキーに関連付けられたリソースに固有です。また、Voice Connector は RetireGrantオペレーションを使用して、リソースを削除するときにグラントを削除します。

次の例では、 CreateGrantオペレーションを記録します。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-04-22T17:02:00Z"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
```

```
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
       "constraints": {
            "encryptionContextSubset": {
                "aws:chime:voice-profile-domain:arn": "arn:aws:chime:us-
west-2:111122223333:voice-profile-domain/sample-domain-id"
            }
        },
        "retiringPrincipal": "chimevoiceconnector.region.amazonaws.com",
        "operations": [
            "GenerateDataKey",
            "Decrypt",
            "DescribeKey",
            "RetireGrant"
        ],
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "granteePrincipal": "chimevoiceconnector.region.amazonaws.com",
        "retiringPrincipal": "chimevoiceconnector.region.amazonaws.com"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

GenerateDataKey

音声プロファイルドメインを作成し、カスタマーマネージドキーをドメインに割り当てると、関連付けられた Voice Connector によって一意のデータキーが作成され、各スピーカーの登録音声が暗号化されます。Voice Connector は、リソースのキーを指定するGenerateDataKeyリクエストを AWS KMS に送信します。

次の例では、 GenerateDataKeyオペレーションを記録します。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionContext": {
            "aws:chime:voice-profile-domain:arn": "arn:aws:chime:us-
west-2:111122223333:voice-profile-domain/sample-domain-id"
        },
        "keySpec": "AES_256",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
```

```
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "sharedEventID": "57f5dbee-16da-413e-979f-2c4c6663475e"
}
```

Decrypt

新しい音声認識モデルのために音声プロファイルドメインの音声プロファイルをアップグレードする必要がある場合、関連付けられた Voice Connector は Decryptオペレーションを呼び出して、保存された暗号化データキーを使用して暗号化されたデータにアクセスします。

次の例では、 Decryptオペレーションを記録します。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-10-12T23:59:34Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionContext": {
            "keyId": "arn:aws:kms:us-
west-2:111122223333:key/44444444-3333-2222-1111-EXAMPLE11111",
            "encryptionContext": {
                "aws:chime:voice-profile-domain:arn": "arn:aws:chime:us-
west-2:111122223333:voice-profile-domain/sample-domain-id"
            },
            "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
        },
        "responseElements": null,
        "requestID": "ed0fe4ab-305b-4388-8adf-7e8e3a4e80fe",
        "eventID": "31d0d7c6-ce5b-4caf-901f-025bf71241f6",
        "readOnly": true,
        "resources": [{
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
```

```
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/00000000-1111-2222-3333-9999999999999"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
        "sharedEventID": "35d58aa1-26b2-427a-908f-025bf71241f6",
        "eventCategory": "Management"
    }
```

DescribeKey

Voice Connector は、 DescribeKeyオペレーションを使用して、音声プロファイルドメインに関連付けられたキーがアカウントとリージョンに存在することを確認します。

次の例では、 DescribeKeyオペレーションを記録します。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-04-22T17:02:00Z"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
```

```
    "eventName": "DescribeKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "keyId": "00dd0db0-0000-0000-ac00-b0c000SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

サービス間の混乱した代理の防止

不分別な代理処理問題とは、アクションを実行する権限のないエンティティが、権限のあるエンティティにアクションを実行するように 呼び出し をすることで発生する情報セキュリティ上の問題です。これにより、悪意のあるアクターが本来であれば実行またはアクセスの権限がないコマンドを実行したり、リソースを変更することが可能になります。詳細については、「AWS Identity and Access Management ユーザーガイド」の「混乱する代理問題」を参照してください。

AWSでは、クロスサービスでのなりすましは混乱した副シナリオにつながります。クロスサービスでのなりすましとは、あるサービス (呼び出し側のサービス) が別のサービス (呼び出しされた側のサービス) を呼び出すときに発生します。悪意のあるアクターは、呼び出し元のサービスを使用して、通常持っていない許可を使用して、別のサービスのリソースを変更できます。

AWS は、アカウント上のリソースへのアクセスの管理をサービスプリンシパルに提供し、リソースのセキュリティを保護できるようにします。リソースポリシーには、aws:SourceAccount のグ

ローバル条件コンテキストキーを使用することをお勧めします。これらのキーは、Amazon Chime SDK がそのリソースに別のサービスに付与するアクセス許可を制限します。

次の例は、設定済みの CallDetailRecords S3 バケット内の aws:SourceAccount グローバル条件コンテキストを使用して混乱する代理問題を防止する S3 バケットポリシーを示しています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonChimeAclCheck668426",
            "Effect": "Allow",
            "Principal": {
                "Service": "chime.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::your-cdr-bucket"
        },
        {
            "Sid": "AmazonChimeWrite668426",
            "Effect": "Allow",
            "Principal": {
                "Service": "chime.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::your-cdr-bucket/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": "112233446677"
                }
            }
        }
    ]
}
```

Amazon Chime SDK リソースベースのポリシー

Amazon Chime SDK は、次のリソースタイプ のリソースベースのポリシーをサポートしています。

Amazon Chime SDK タグに基づく認可

Amazon Chime SDK は、これらのリソースタイプ のタグ付けをサポートしています。

Amazon Chime SDK IAM ロール

IAM ロールは AWS アカウント内のエンティティで、特定の許可を持っています。

Amazon Chime SDK での一時的な認証情報の使用

一時的な認証情報を使用して、フェデレーションでサインインする、IAM ロールを引き受ける、またはクロスアカウントロールを引き受けることができます。一時的なセキュリティ認証情報を取得するには、 AssumeRole や GetFederationToken などの AWS STS API オペレーションを呼び出します。

Amazon Chime SDK は、一時的な認証情報の使用をサポートしています。

サービスにリンクされたロール

サービスリンクロールによって、AWS サービスが他のサービスのリソースにアクセスしてユーザーに代わってアクションを完了する事ができます。サービスリンクロールは、IAM アカウント内に表示され、ロールをはサービスによって所有されます。IAM 管理者はサービスリンク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。

Amazon Chime SDK は、サービスにリンクされたロールをサポートしています。これらのロールの作成または管理の詳細については、「」を参照してくださいAmazon Chime SDK のサービスにリンクされたロールの使用。

サービスロール

この機能により、ユーザーに代わってサービスがサービスロールを引き受けることが許可されます。このロールにより、サービスがお客様に代わって他のサービスのリソースにアクセスし、アクションを完了することが許可されます。サービスロールは、IAM アカウントに表示され、アカウントによって所有されます。つまり、IAM 管理者は、このロールの権限を変更できます。ただし、それにより、サービスの機能が損なわれる場合があります。

Amazon Chime SDK はサービスロールをサポートしていません。

Amazon Chime SDK 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、IAM ユーザーおよびロールには Amazon Chime SDK 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 Management Console、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、管理者はそれらの権限が必要な IAM ユーザーまたはグループにそのポリシーをアタッチする必要があります。

これらの JSON ポリシードキュメント例を使用して IAM の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

アイデンティティベースポリシーは非常に強力です。アカウント内で誰かが Amazon Chime SDK 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を使用して開始する – Amazon Chime SDK の使用をすばやく開始するには、 AWSマネージドポリシーを使用して、従業員に必要なアクセス許可を付与します。これらのポリシーはアカウントで既に有効になっており、AWS によって管理および更新されています。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使用した許可の使用スタート」を参照してください。
- 最小特権を付与する - カスタムポリシーを作成するときは、タスクの実行に必要な許可のみを付与します。最小限の許可からスタートし、必要に応じて追加の許可を付与します。この方法は、寛容過ぎる許可から始めて、後から厳しくしようとするよりも安全です。詳細については、IAM ユーザーガイドの「最小特権を認める」を参照してください。

- 機密性の高いオペレーションに MFA を有効にする - 追加セキュリティとして、機密性の高いリソースまたは API オペレーションにアクセスするために IAM ユーザーに対して、多要素認証 (MFA) の使用を要求します。詳細については、IAM ユーザーガイドの「AWS での多要素認証 (MFA) の使用」を参照してください。
- 追加のセキュリティとしてポリシー条件を使用する - 実行可能な範囲内で、アイデンティティベースのポリシーがリソースへのアクセスを許可する条件を定義します。例えば、あるリクエストの送信が許可される IP アドレスの範囲を指定するための条件を記述できます。指定された日付または時間範囲内でのみリクエストを許可する条件を書くことも、SSL や MFA の使用を要求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。

AWS マネージド Amazon Chime SDK ポリシー

AWS マネージドAmazonChimeVoiceConnectorServiceLinkedRoleポリシーを使用して、Amazon Chime SDK アクションへのアクセス権をユーザーに付与します。詳細については、「Amazon Chime SDK デベロッパーガイド」の「IAM ロールの例」、および「サービス認証リファレンス」の「Amazon Chime 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。

```
// Policy ARN: arn:aws:iam::aws:policy/AmazonChimeSDK
// Description: Provides access to Amazon Chime SDK operations
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "chime:CreateMediaCapturePipeline",
                "chime:CreateMediaConcatenationPipeline",
                "chime:CreateMediaLiveConnectorPipeline",
                "chime:CreateMeeting",
                "chime:CreateMeetingWithAttendees",
                "chime:DeleteMediaCapturePipeline",
                "chime:DeleteMediaPipeline",
                "chime:DeleteMeeting",
                "chime:GetMeeting",
                "chime:ListMeetings",
                "chime:CreateAttendee",
                "chime:BatchCreateAttendee",
                "chime:DeleteAttendee",
                "chime:GetAttendee",
                "chime:GetMediaCapturePipeline",
```

```
                "chime:GetMediaPipeline",
                "chime:ListAttendees",
                "chime:ListAttendeeTags",
                "chime:ListMediaCapturePipelines",
                "chime:ListMediaPipelines",
                "chime:ListMeetingTags",
                "chime:ListTagsForResource",
                "chime:StartMeetingTranscription",
                "chime:StopMeetingTranscription",
                "chime:TagAttendee",
                "chime:TagMeeting",
                "chime:TagResource",
                "chime:UntagAttendee",
                "chime:UntagMeeting",
                "chime:UntagResource"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS マネージドポリシー: AmazonChimeVoiceConnectorServiceLinkedRoleポリシー

AmazonChimeVoiceConnectorServiceLinkedRolePolicy を使用すると、Amazon Chime SDK Voice Connector は Amazon Kinesis Video Streams にメディアをストリーミングし、ストリーミング通知を提供し、Amazon Polly を使用して音声を合成できます。このポリシーは、Amazon Chime SDK Voice Connector サービスに、お客様の Amazon Kinesis Video Streams へのアクセス、Amazon Simple Notification Service (SNS) と Amazon Simple Queue Service (SQS) への通知イベントの送信、Amazon Polly を使用した Amazon Chime SDK Voice Applications and SpeakAndGetDigits Actions を使用する際の音声の合成を行うためのアクセス許可を付与Speakします。

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

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "kinesisvideo:GetDataEndpoint",
                "kinesisvideo:PutMedia",
                "kinesisvideo:UpdateDataRetention",
                "kinesisvideo:DescribeStream",
                "kinesisvideo:CreateStream"
            ],
            "Resource": ["arn:aws:kinesisvideo:*:*:stream/ChimeVoiceConnector-*"]
        },
        {
            "Effect": "Allow",
            "Action": ["kinesisvideo:ListStreams"],
            "Resource": ["*"]
        },
        {
            "Effect": "Allow",
            "Action": ["SNS:Publish"],
            "Resource": ["arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"]
        },
        {
            "Effect": "Allow",
            "Action": ["sqs:SendMessage"],
            "Resource": ["arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"]
        },
        {
            "Effect": "Allow",
            "Action": ["polly:SynthesizeSpeech"],
            "Resource": ["*"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "chime:CreateMediaInsightsPipeline",
                "chime:GetMediaInsightsPipelineConfiguration"
            ],
            "Resource": ["*"]
        }
    ]
}
```

詳細については、「Amazon Chime SDK Voice Connector サービスにリンクされたロールポリシーの使用」を参照してください。

AWS マネージドポリシー: AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

IAM エンティティに AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy をアタッチすることはできません。

このポリシーにより、Kinesis Video Streams は Amazon Chime SDK 会議にデータをストリーミングし、 にメトリクスを発行できます CloudWatch。また、Amazon Chime SDK メディアパイプラインがユーザーに代わって Amazon Chime SDK 会議にアクセスすることもできます。詳細については、このガイドの「Amazon Chime SDK メディアパイプラインでのロールの使用」を参照してください。

権限の詳細

このポリシーには、以下の権限が含まれています。

- cloudwatch – CloudWatch メトリクスを配置するアクセス許可を付与します。
- kinesisvideo – データエンドポイントの取得、メディアの配置、データ保持期間の更新、データストリームの記述、データストリームの作成、データストリームの一覧表示を行うアクセス許可を付与します。
- chime - 会議の取得、参加者の作成、参加者の削除を行うアクセス許可を付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPutMetricsForChimeSDKNamespace",
            "Effect": "Allow",
            "Action": "cloudwatch:PutMetricData",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/ChimeSDK"
                }
            }
        },
```

```
        {
            "Sid": "AllowKinesisVideoStreamsAccess",
            "Effect": "Allow",
            "Action": [
                "kinesisvideo:GetDataEndpoint",
                "kinesisvideo:PutMedia",
                "kinesisvideo:UpdateDataRetention",
                "kinesisvideo:DescribeStream",
                "kinesisvideo:CreateStream"
            ],
            "Resource": [
                "arn:aws:kinesisvideo:*:*:stream/ChimeMediaPipelines-*"
            ]
        },
        {
            "Sid": "AllowKinesisVideoStreamsListAccess",
            "Effect": "Allow",
            "Action": [
                "kinesisvideo:ListStreams"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "AllowChimeMeetingAccess",
            "Effect": "Allow",
            "Action": [
                "chime:GetMeeting",
                "chime:CreateAttendee",
                "chime:DeleteAttendee"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS マネージドポリシーに対する Amazon Chime 更新

次の表は、Amazon Chime SDK IAM ポリシーに加えられた更新のリストと説明です。

変更	説明	日付
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy – 既存のポリシーの更新	Amazon Chime SDK 会議が にメトリクスを公開してサービスダッシュボード CloudWatch で使用できるようにするアクセス許可`AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy` が追加されました。詳細については、「Amazon Chime SDK メディアパイプラインでのロールの使用」を参照してください。	2023 年 12 月 8 日
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy – 既存のポリシーの更新	Kinesis Video Streams が Amazon Chime SDK 会議にオーディオ、ビデオ、および画面共有データをストリーミングできるようにするアクセス許可`AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy` が追加されました。詳細については、「Amazon Chime SDK メディアパイプラインでのロールの使用」を参照してください。	2023 年 8 月 20 日
AmazonChimeVoiceConnectorServiceLinkedRoleポリシー – 既存のポリシーへの更新	GetMediaInsightsPipelineConfiguration API へのアクセスを許可するアクセス許可`AmazonChimeVoiceConnectorServiceLinkedRolePolicy` が追加されました。Amazon Chime Voice	2023 年 4 月 14 日

変更	説明	日付
	Connector では、メディアインサイトパイプライン設定を取得するために、これらのアクセス許可が必要です。詳細については、「通話分析を使用するための Voice Connector の設定」を参照してください。	
新規および更新されたサービスにリンクされたロール	デベロッパーは AmazonChimeSDKEvents サービスにリンクされたロールを使用して、Kinesis Firehose などのストリーミングサービスにアクセスできます。詳細については、「 AmazonChimeSDKEvents サービスにリンクされたロールの使用」を参照してください。また、「サービスにリンクされたロールの使用」にAmazonChimeVoiceConnectorServiceLinkedRoleポリシー名を追加しました。詳細については、「 AmazonChimeVoiceConnectorServiceLinkedRoleポリシーの使用」を参照してください。	2023 年 3 月 27 日

変更	説明	日付
Amazon Chime SDK アイデンティティベースのポリシーの例 — 既存のポリシーへの更新。	AWS マネージド Amazon Chime SDK ポリシーに、Amazon Chime SDK Media Pipeline APIs を使用してメディアパイプラインを作成、読み取り、削除できるアクセス許可が追加されました。	2023 年 1 月 5 日
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy – 新しい マネージドポリシーを追加しました。	Amazon Chime SDK に、Amazon Chime SDK 会議でメディアキャプチャパイプラインを使用できるようにするサービスリンクロールが追加されました。	2022 年 4 月 27 日
AWS マネージドポリシー: AmazonChimeVoiceConnectorServiceLinkedRoleポリシー – 既存のポリシーへの更新。	Amazon Chime SDK Voice Connector に、Amazon Polly を使用して音声を合成するためのアクセス許可が追加されました。これらのアクセス許可は、Amazon Chime SDK Voice Applications で `Speak`および `SpeakAndGetDigits` アクションを使用するために必要です。	2022 年 3 月 15 日

変更	説明	日付
AmazonChimeVoiceConnectorServiceLinkedRoleポリシー – 既存のポリシーへの更新	Amazon Chime SDK Voice Connector に、Amazon Kinesis Video Streams へのアクセスと、Amazon Simple Notification Service (Amazon SNS) および Amazon Simple Query Service (Amazon SQS) への通知イベントの送信を許可するアクセス許可が追加されました。これらのアクセス許可は、Amazon Chime SDK Voice Connector が Amazon Kinesis Video Streams にメディアをストリーミングし、ストリーミング通知を提供するために必要です。	2021 年 12 月 20 日
既存のポリシー関する変更。Amazon Chime SDK ポリシーを使用した IAM ユーザーまたはロールの作成。	Amazon Chime SDK に、拡張検証をサポートする新しいアクションが追加されました。 出席者と会議リソースの一覧表示とタグ付けが可能になり、会議の文字起こしを開始および停止するためのアクションが追加されました。	2021 年 9 月 23 日
Amazon Chime SDK が変更の追跡を開始	Amazon Chime SDK が AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 9 月 23 日

Amazon Chime SDK 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

以下の情報は、Amazon Chime SDK 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復に役立ちます。

トピック

Amazon Chime SDK でアクションを実行する権限がない

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、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。

次の例は、mateojackson という IAM ユーザーがコンソールを使用して架空の *my-example-widget* リソースに関する詳細を表示しようとしたとき、架空の chime:*GetWidget* アクセス許可がない場合に発生するエラーを示しています。

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

この場合、chime:*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 管理者に問い合わせてください。管理者とは、サインイン認証情報を提供した担当者です。

iam を実行する権限がありません。PassRole

iam:PassRole アクションを実行することが認可されていないというエラーが表示された場合、管理者に問い合わせ、サポートを依頼する必要があります。管理者は、ユーザー名とパスワードを提供した人です。Amazon Chime SDK 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よう、管理者に依頼します。

一部の AWS サービスでは、新しいサービスロールまたはサービスリンクロールを作成せずに、既存のロールをサービスに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許可が必要です。

以下の例のエラーは、 という名前の IAM `marymajor` ユーザーが サービスを使用して Amazon Chime SDK でアクションを実行しようする場合に発生します。ただし、アクションには、サービスロールによってサービスに許可が付与されている必要があります。Mary には、ロールをサービスに渡す許可がありません。

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

この場合、Mary は `iam:PassRole` アクションの実行が許可されるように、担当の管理者にポリシーの更新を依頼します。

Amazon Chime SDK のサービスにリンクされたロールの使用

Amazon Chime SDK は、AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは、Amazon Chime SDK に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは、Amazon Chime SDK によって事前定義されており、ユーザーに代わってサービスから他の AWSのサービスを呼び出す必要のあるアクセス許可がすべて含まれています。

サービスにリンクされたロールを使用することで、必要なアクセス許可を手動で追加する必要がなくなるため、Amazon Chime SDK の設定がより効率的になります。Amazon Chime SDK は、サービスにリンクされたロールのアクセス許可を定義します。特に定義されている場合を除き、Amazon Chime SDK のみがそのロールを引き受けることができます。定義されたアクセス許可には、信頼ポリシーとアクセス許可ポリシーが含まれます。アクセス許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスリンクロールは、まずその関連リソースを削除しなければ削除できません。これは、リソースにアクセスするための許可を誤って削除できないため、Amazon Chime SDK リソースを保護します。

サービスリンクロールをサポートしているその他のサービスの詳細については、「IAM と連携する AWS のサービス」を参照してください。[サービスにリンクロール] 列が「はい」になっている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。

トピック

- Amazon Chime SDK Voice Connector サービスにリンクされたロールポリシーの使用
- ライブトランスクリプション (ライブでの文字起こし) でロールを使用する

- Amazon Chime SDK メディアパイプラインでのロールの使用
- AmazonChimeSDKEvents サービスにリンクされたロールの使用

Amazon Chime SDK Voice Connector サービスにリンクされたロールポリシーの使用

以下のセクションでは、次の方法について説明します。

- Amazon Chime SDK Voice Connector サービスにリンクされたロールポリシーを使用して、Amazon Chime SDK Voice Connector メディアを Kinesis にストリーミングします。
- Amazon Polly と発話 および SpeakAndGetDigitsアクションを使用して音声を合成します。

トピック

- Amazon Chime SDK Voice Connector のサービスにリンクされたロールのアクセス許可
- Amazon Chime SDK Voice Connector のサービスにリンクされたロールの作成
- Amazon Chime SDK Voice Connector のサービスにリンクされたロールの編集
- Amazon Chime SDK Voice Connector のサービスにリンクされたロールの削除
- Amazon Chime SDK のサービスにリンクされたロールがサポートされるリージョン

Amazon Chime SDK Voice Connector のサービスにリンクされたロールのアクセス許可

Amazon Chime SDK Voice Connector は、 という名前のサービスにリンクされたロールを使用しますAWSServiceRoleForAmazonChimeVoiceConnector。これにより、Amazon Chime SDK Voice Connector はユーザーに代わって AWSのサービスを呼び出すことができます。Amazon Chime SDK Voice Connector のメディアストリーミングを開始する方法の詳細については、「」を参照してくださいAmazon Chime SDK Voice Connector メディアを Kinesis にストリーミングする。

AWSServiceRoleForAmazonChimeVoiceConnector サービスにリンクされたロールは、以下のサービスを信頼してロールを引き受けます。

- `voiceconnector.chime.amazonaws.com`

AmazonChimeVoiceConnectorServiceLinkedRoleポリシーにより、Amazon Chime SDK は指定されたリソースに対して以下のアクションを実行できます。

- アクション: `all AWS resources` 上で `chime:GetVoiceConnector*`
- アクション: `arn:aws:kinesisvideo:us-east-1:111122223333:stream/ChimeVoiceConnector-*` 上で `kinesisvideo:*`
- アクション: `all AWS resources` 上で `polly:SynthesizeSpeech`
- アクション: `all AWS resources` 上で `chime:CreateMediaInsightsPipeline`
- アクション: `all AWS resources` 上で `chime:GetMediaInsightsPipelineConfiguration`
- アクション: `arn:aws:kinesisvideo:us-east-1:111122223333:stream/ChimeMediaPipelines-*` 上で `kinesisvideo:CreateStream`
- アクション: `arn:aws:kinesisvideo:us-east-1:111122223333:stream/ChimeMediaPipelines-*` 上で `kinesisvideo:PutMedia`
- アクション: `arn:aws:kinesisvideo:us-east-1:111122223333:stream/ChimeMediaPipelines-*` 上で `kinesisvideo:UpdateDataRetention`
- アクション: `arn:aws:kinesisvideo:us-east-1:111122223333:stream/ChimeMediaPipelines-*` 上で `kinesisvideo:DescribeStream`
- アクション: `arn:aws:kinesisvideo:us-east-1:111122223333:stream/ChimeMediaPipelines-*` 上で `kinesisvideo:GetDataEndpoint`
- アクション: `kinesisvideo:ListStreams` 上で `arn:aws:kinesisvideo:us-east-1:111122223333:stream/*`

サービスにリンクされたロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、権限を設定する必要があります。詳細については、「IAM ユーザーガイド」の「サービスリンクロール権限」を参照してください。

Amazon Chime SDK Voice Connector のサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。Amazon Chime SDK Voice Connector の Kinesis メディアストリーミングを開始するか、AWS Management Console、、または AWS API で Amazon Chime SDK SIP メディアアプリケーションを作成AWS CLIまたは更新すると、Amazon Chime によってサービスにリンクされたロールが作成されます。

IAM コンソールで Chime Voice Connector ユースケースによるサービスリンクロールを作成することもできます。AWS CLI または AWS API では、`voiceconnector.chime.amazonaws.com` サービス名を使用してサービスにリンクされた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「サービスにリンクされたロールの作成」を参照してください。このサービスにリンクされたロールを削除しても、この同じプロセスを使用して、もう一度ロールを作成できます。

Amazon Chime SDK Voice Connector のサービスにリンクされたロールの編集

Amazon Chime SDK では、 AWSServiceRoleForAmazonChimeVoiceConnector サービスにリンクされたロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、『IAM ユーザーガイド』の「サービスにリンクされたロールの編集」を参照してください。

Amazon Chime SDK Voice Connector のサービスにリンクされたロールの削除

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスリンクロールのクリーンアップ

IAM を使用してサービスリンクロールを削除するには、最初に、そのロールで使用されているリソースをすべて削除する必要があります。

> **Note**
>
> リソースを削除する際に Amazon Chime SDK サービスでロールが使用されている場合、削除は失敗することがあります。失敗した場合は、数分待ってから操作を再試行してください。

で使用されている Amazon Chime SDK リソースを削除するには AWSServiceRoleForAmazonChimeVoiceConnector（コンソール）

- Amazon Chime SDK アカウント内のすべての Amazon Chime SDK Voice Connector のメディアストリーミングを停止します。
  a. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
  b. ナビゲーションペインの SIP Trunking で、音声コネクタ を選択します。

c. Amazon Chime SDK Voice Connector の名前を選択します。
d. ストリーミングタブを選択します。
e. 「Kinesis Video Streams に送信」で、「停止」を選択します。
f. [Save] (保存) を選択します。

で使用されている Amazon Chime SDK リソースを削除するには AWSServiceRoleForAmazonChimeVoiceConnector（ AWS CLI)

- CLI の AWS delete-voice-connector-streaming-configuration コマンドを使用して、アカウント内のすべての Amazon Chime SDK Voice Connector のメディアストリーミングを停止します。

```
aws chime delete-voice-connector-streaming-configuration --voice-connector-
id abcdef1ghij2klmno3pqr4
```

AWSServiceRoleForAmazonChimeVoiceConnector (API) で使用されている Amazon Chime SDK リソースを削除するには

- DeleteVoiceConnectorStreamingConfiguration API を使用して、アカウント内のすべての Amazon Chime SDK Voice Connector のメディアストリーミングを停止します。

サービスにリンクされたロールを手動で削除する

IAM コンソール、AWS CLI、または AWS API オペレーションを使用して、AWSServiceRoleForAmazonChimeVoiceConnector サービスにリンクされたロールを削除します。詳細については、IAM ユーザーガイド の「サービスリンクロールの削除」を参照してください。

Amazon Chime SDK のサービスにリンクされたロールがサポートされるリージョン

Amazon Chime SDK は、このサービスを利用できるすべての AWS リージョンで、サービスにリンクされたロールの使用をサポートします。詳細については、「Amazon Chime エンドポイントとクォータ」を参照してください。

ライブトランスクリプション (ライブでの文字起こし) でロールを使用する

以下のセクションでは、Amazon Chime SDK ライブ文字起こしのサービスリンクロールを作成および管理する方法について説明します。ライブトランスクリプションサービスの詳細については、「Amazon Chime SDK ライブトランスクリプションの使用」を参照してください。

トピック

Amazon Chime SDK ライブトランスクリプションのサービスリンクロール許可

Amazon Chime SDK Live Transcription は、 というAWSServiceRoleForAmazonChimeTranscription 名前のサービスにリンクされたロールを使用します。これにより、Amazon Chime SDK がユーザーに代わって Amazon Transcribe と Amazon Transcribe Medical にアクセスできるようになります。

AWSServiceRoleForAmazonChimeTranscription サービスにリンクされたロールは、以下のサービスを信頼してロールを引き受けます。

- `transcription.chime.amazonaws.com`

ロールのアクセス許可ポリシーにより、Amazon Chime SDK は指定されたリソースに対して以下のアクションを実行できます。

- アクション: `all AWS resources` 上で `transcribe:StartStreamTranscription`
- アクション: `transcribe:StartMedicalStreamTranscription` 上で `all AWS resources`

サービスにリンクされたロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、権限を設定する必要があります。詳細については、「IAM ユーザーガイド」の「サービスリンクロール権限」を参照してください。

Amazon Chime SDK ライブトランスクリプションのサービスリンクロールの作成

IAM コンソールで Chime Transcription ユースケースによるサービスリンクロールを作成できます。

> **Note**
>
> これらのステップを完了するには、IAM 管理者権限が必要です。お持ちでない場合、システム管理者に相談してください。

ロールを作成するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. IAM コンソールのナビゲーションペインで [Roles] (ロール)、[Create role] (ロールの作成) の順に選択します。
3. [AWS Service] (AWS のサービス) ロールタイプを選択してから [Chime Transcription] を選択します。

   IAM ポリシーが表示されます。
4. ポリシーの横にあるチェックボックスをオンにしてから [Next: Tags] (次へ: タグ) を選択します。
5. [Next: Review] (次へ: 確認) を選択します。
6. 必要に応じて説明を編集してから [Create role] (ロールの作成) を選択します。

AWS CLI または AWS API を使用して transcription.chime.amazonaws.com というサービスリンクロールを作成することもできます。

CLI で `aws iam create-service-linked-role --aws-service-name transcription.chime.amazonaws.com` コマンドを実行します。

詳細については、IAM ユーザーガイドの「サービスリンクロールの作成」を参照してください。このサービスにリンクされたロールを削除しても、この同じプロセスを使用して、もう一度ロールを作成できます。

Amazon Chime SDK ライブトランスクリプションのサービスリンクロールの編集

Amazon Chime SDK では、 AWSServiceRoleForAmazonChimeTranscription サービスにリンクされたロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用してロールの説明を編集することはできます。詳細については、IAM ユーザーガイドの「サービスリンクロールの編集」を参照してください。

Amazon Chime SDK ライブトランスクリプションのサービスリンクロールの削除

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。

サービスにリンクされたロールを IAM で手動削除するには

IAM コンソール、AWS CLI、または AWS API を使用して、AWSServiceRoleForAmazonChimeTranscription サービスリンクロールを削除します。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの削除」を参照してください。

Amazon Chime のサービスリンクロールがサポートされるリージョン

Amazon Chime SDK は、このサービスを利用できるすべてのリージョンで、サービスにリンクされたロールの使用をサポートします。詳細については、「Amazon Chime エンドポイントとクォータ」および「Amazon Chime SDK メディアリージョンの使用」を参照してください。

Amazon Chime SDK メディアパイプラインでのロールの使用

以下のセクションでは、Amazon Chime SDK メディアパイプラインのサービスリンクロールを作成および管理する方法について説明します。

トピック

- Amazon Chime SDK メディアパイプラインのサービスリンクロールアクセス許可
- Amazon Chime SDK メディアパイプラインのサービスリンクロールの作成
- Amazon Chime SDK パイプラインのサービスリンクロールの編集
- Amazon Chime SDK メディアパイプラインのサービスリンクロールの削除
- Amazon Chime SDK メディアパイプラインのサービスリンクロールがサポートされるリージョン

Amazon Chime SDK メディアパイプラインのサービスリンクロールアクセス許可

Amazon Chime SDK は、 という名前のサービスにリンクされたロールを使用します。AWSServiceRoleForAmazonChimeSDKMediaPipelinesこれにより、Amazon Chime SDK メディアパイプラインがユーザーに代わって AWSサービスにアクセスできるようになります。

AWSServiceRoleForAmazonChimeSDKMediaPipelines サービスにリンクされたロールは、ロールの引き受けについて以下のサービスを信頼します。

- `mediapipelines.chime.amazonaws.com`

このロールにより、Amazon Chime SDK は指定されたリソースに対して以下のアクションを実行できます。

- アクション: all AWS resources 上で cloudwatch:PutMetricData
- アクション: all AWS resources 上で chime:CreateAttendee
- アクション: all AWS resources 上で chime:DeleteAttendee
- アクション: all AWS resources 上で chime:GetMeeting
- アクション: arn:aws:kinesisvideo:*:*111122223333*:stream/ChimeMediaPipelines-* 上で kinesisvideo:CreateStream
- アクション: arn:aws:kinesisvideo:*:*111122223333*:stream/ChimeMediaPipelines-* 上で kinesisvideo:PutMedia
- アクション: arn:aws:kinesisvideo:*:*111122223333*:stream/ChimeMediaPipelines-* 上で kinesisvideo:UpdateDataRetention
- アクション: arn:aws:kinesisvideo:*:*111122223333*:stream/ChimeMediaPipelines-* 上で kinesisvideo:DescribeStream
- アクション: arn:aws:kinesisvideo:*:*111122223333*:stream/ChimeMediaPipelines-* 上で kinesisvideo:GetDataEndpoint
- アクション: kinesisvideo:ListStreams 上で arn:aws:kinesisvideo:*:*111122223333*:stream/*

サービスにリンクされたロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、権限を設定する必要があります。アクセス許可の設定の詳細については、IAM ユーザーガイドの「サービスにリンクされたロールのアクセス許可」を参照してください。

の詳細についてはAmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy、このガイドの前半にあるAWS マネージドポリシー: AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy「」を参照してください。

Amazon Chime SDK メディアパイプラインのサービスリンクロールの作成

IAM コンソールを使用して、Amazon Chime SDK Media Pipelines ユースケースでサービスにリンクされたロールを作成します。

> **Note**
>
> これらのステップを完了するには、IAM 管理者権限が必要です。お持ちでない場合、システム管理者に相談してください。

ロールを作成するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. IAM コンソールのナビゲーションペインで [Roles] (ロール)、[Create role] (ロールの作成) の順に選択します。
3. [AWS のサービス] ロールタイプを選択してから [Chime] を選択し、次に [Chime SDK メディアパイプライン] を選択します。
4. [次へ] をクリックします。
5. [次へ] をクリックします。
6. 必要に応じて説明を編集してから [Create role] (ロールの作成) を選択します。

AWS CLI または AWS API を使用して、 という名前のサービスにリンクされたロールを作成することもできますmediapipelines.chime.amazonaws.com。

AWS CLI でこのコマンドを実行します: **`aws iam create-service-linked-role --aws-service-name mediapipelines.chime.amazonaws.com`**

詳細については、IAM ユーザーガイドの「サービスリンクロールの作成」を参照してください。このサービスにリンクされたロールを削除しても、この同じプロセスを使用して、もう一度ロールを作成できます。

Amazon Chime SDK パイプラインのサービスリンクロールの編集

Amazon Chime SDK では、AWSServiceRoleForAmazonChimeSDKMediaPipelinesサービスにリンクされたロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

Amazon Chime SDK メディアパイプラインのサービスリンクロールの削除

サービスにリンクされたロールを必要とする機能やサービスを使用する必要がない場合は、そのロールを削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングまたはメンテナンスされることがなくなります。

サービスにリンクされたロールを IAM で手動削除するには

IAM コンソール、AWS CLI、または AWS API を使用して、AWSServiceRoleForAmazonChimeSDKMediaPipelines サービスリンクロールを削除します。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの削除」を参照してください。

Amazon Chime SDK メディアパイプラインのサービスリンクロールがサポートされるリージョン

Amazon Chime SDK は、このサービスを利用できるすべてのAWSリージョンで、サービスにリンクされたロールの使用をサポートします。詳細については、「Amazon Chime エンドポイントとクォータ」を参照してください。

AmazonChimeSDKEvents サービスにリンクされたロールの使用

Amazon Chime SDK は、 という名前のサービスにリンクされたロールを使用しますAmazonChimeSDKEvents。このロールは、データストリーミングに使用される Kinesis Firehose など、Amazon Chime SDK が使用または管理する AWSサービスとリソースへのアクセスを許可します。

AmazonChimeSDKEvents サービスにリンクされたロールにより、Amazon Chime SDK は kinesis:PutRecordと の形式のストリームkinesis:PutRecordBatchを完了できますarn:aws:firehose:::deliverystream/AmazonChimeSDKEvents-*。

サービスにリンクされたロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、「IAM User Guide」(IAM ユーザーガイド) の「Service-linked role permissions」(サービスにリンクされたロールのアクセス権限) を参照してください。

サービスにリンクされたロールの作成

サービスにリンクされたロールは、クイック作成リンクの Chime SDK Events CloudFormation テンプレートの一部です。

IAM コンソールを使用して、Amazon Chime SDK Events ユースケースでサービスにリンクされたロールを作成することもできます。AWS CLI または AWS API で、サービスにリンクされたロールをサービス名 events.chime.amazonaws.com で作成します。詳細については、「 IAM ユーザーガイド」の「サービスにリンクされたロールの使用」を参照してください。このロールを削除しても、このプロセスを繰り返して再度作成することができます。

サービスにリンクされたロールの編集

サービスにリンクされたロールの作成後は、その説明のみ編集できます。編集は IAM を使用して行います。詳細については、「 IAM ユーザーガイド」の「サービスにリンクされたロールの使用」を参照してください。

サービスにリンクされたロールの削除

ベストプラクティスとして、Amazon Chime SDKEventsロールを必要とする機能やサービスが不要になった場合は、ロールを削除してください。そうしないと、アクティブにモニタリングもメンテナンスもされない不使用のエンティティが存在することになります。

ロールを手動で削除するには、まずロールが使用するリソースを削除します。以下のステップでは、両方のタスクを実行する方法を説明します。

ロールリソースの削除

リソースを削除するには、データのストリーミングに使用される Kinesis Firehose を削除します。

> **Note**
>
> ロールがリソースを使用しているときにリソースを削除しようとすると、削除が失敗する可能性があります。削除が失敗した場合は、数分待ってから操作を再試行してください。

ロールリソースを削除するには

- 次の API を呼び出して、Kinesis Firehose をオフにします。

```
aws firehose delete-delivery-stream --delivery-stream-name delivery_stream_name
```

サービスにリンクされたロールを削除するには

- IAM コンソール、CLI、または AWS API AWS を使用して、 AmazonChimeSDKEvents サービスにリンクされたロールを削除します。詳細については、IAM ユーザーガイドの「サービスにリンクされたロールの使用」および「サービスにリンクされたロールの削除」を参照してください。

Amazon Chime SDK でのログ記録とモニタリング

モニタリングは、Amazon Chime SDK およびその他の AWSソリューションの信頼性、可用性、およびパフォーマンスを維持する上で重要な部分です。 AWSには、Amazon Chime SDK をモニタリングし、問題を報告して、必要に応じて自動アクションを実行するための以下のツールが用意されています。

- Amazon CloudWatch は、 AWSリソースと で実行しているアプリケーションをリアルタイムでモニタリングしますAWS。メトリクスを収集および追跡し、カスタマイズされたダッシュボードを作成し、指定されたメトリックが指定したしきい値に達したときに通知またはアクションを実行するアラームを設定できます。例えば、 で Amazon EC2 インスタンスの CPU 使用率やその他のメトリクス CloudWatch を追跡し、必要に応じて新しいインスタンスを自動的に起動できます。詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。
- Amazon EventBridge は、 AWSリソースの変更を示すシステムイベントのほぼリアルタイムのストリームを提供します。 は、自動化されたイベント駆動型コンピューティング EventBridge を有効にします。これにより、特定のイベントをモニタリングし、これらのイベントが発生したときに他の AWS サービスで自動アクションをトリガーするルールを記述できます。詳細については、「Amazon ユーザーガイド EventBridge 」を参照してください。
- Amazon CloudWatch Logs では、Amazon EC2 インスタンスやその他のソースからのログファイルをモニタリング、保存 CloudTrail、およびアクセスできます。 CloudWatch Logs はログファイル内の情報をモニタリングし、特定のしきい値に達したときに通知できます。高い耐久性を備えたストレージにログデータをアーカイブすることもできます。詳細については、「Amazon CloudWatch Logs ユーザーガイド」を参照してください。
- AWS CloudTrail は、AWS アカウントによって呼び出されたか、またはそのアカウントに代わって呼び出された API コールとそれに関連するイベントを記録します。次に、指定した Amazon S3 バケットにログファイルが渡されます。AWS を呼び出したユーザーとアカウント、呼び出し元の IP アドレス、および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。

トピック

- Amazon を使用した Amazon Chime SDK のモニタリング CloudWatch
- を使用した Amazon Chime SDK の自動化 EventBridge
- を使用した API コールAWS CloudTrailのログ記録

Amazon を使用した Amazon Chime SDK のモニタリング CloudWatch

CloudWatch を使用して Amazon Chime SDK をモニタリングできます。 は raw CloudWatch データを収集し、リアルタイムに近い読み取り可能なメトリクスに加工します。これらの統計は 15 か月間保持されるため、履歴情報にアクセスしてウェブアプリケーションまたはサービスの動作をより的確に把握できます。また、特定のしきい値をモニタリングするアラームを設定し、しきい値に達したときに通知を送信したりアクションを実行したりできます。詳細については、「Amazon ユーザーガイド CloudWatch 」を参照してください。

CloudWatch Amazon Chime SDK の メトリクス

Amazon Chime SDK は、通話中に 1 CloudWatch 分間に 1 回メトリクスを送信し、ここにリストされているすべてのメトリクスを送信します。

`AWS/ChimeVoiceConnector` 名前空間には、AWSアカウントと Amazon Chime SDK Voice Connector に割り当てられた電話番号に関する以下のメトリクスが含まれます。

> **Note**
>
> SDK は、呼び出し中にパケット損失値を 1 分に 1 回送信します。損失値は、呼び出し中に累積されます。例えば、パケット損失が 11:01 に発生した場合、その損失値は呼び出しの残り分間保持されます。呼び出しの最後に、パケット損失メトリクスが 1 つ表示されます。

メトリクス	説明
`InboundCallAttempts`	試行された受信通話の数。 単位: 回
`InboundCallFailures`	受信通話の失敗回数。 単位: 回
`InboundCallsAnswered`	応答された受信通話の数。 単位: 回
`InboundCallsActive`	現在アクティブな受信通話の数。

メトリクス	説明
	単位: カウント
OutboundCallAttempts	試行された発信通話の数。 単位: カウント
OutboundCallFailures	発信通話の失敗回数。 単位: カウント
OutboundCallsAnswered	応答された発信通話の数。 単位: カウント
OutboundCallsActive	現在アクティブな発信通話の数。 単位: カウント
Throttles	通話の試行時にアカウントがスロットルされる回数。 単位: カウント
Sip1xxCodes	1xx レベルのステータスコードを持つ SIP メッセージの数。 単位: カウント
Sip2xxCodes	2xx レベルのステータスコードを持つ SIP メッセージの数。 単位: カウント
Sip3xxCodes	3xx レベルのステータスコードを持つ SIP メッセージの数。 単位: カウント

メトリクス	説明
Sip4xxCodes	4xx レベルのステータスコードを持つ SIP メッセージの数。 単位: カウント
Sip5xxCodes	5xx レベルのステータスコードを持つ SIP メッセージの数。 単位: カウント
Sip6xxCodes	6xx レベルのステータスコードを持つ SIP メッセージの数。 単位: カウント
CustomerToVcRtpPackets	カスタマーから Amazon Chime SDK Voice Connector インフラストラクチャに送信された RTP パケットの数。 単位: カウント
CustomerToVcRtpBytes	RTP パケットで顧客から Amazon Chime SDK Voice Connector インフラストラクチャに送信されたバイト数。 単位: カウント
CustomerToVcRtcpPackets	顧客から Amazon Chime SDK Voice Connector インフラストラクチャに送信された RTCP パケットの数。 単位: カウント
CustomerToVcRtcpBytes	RTCP パケットで顧客から Amazon Chime SDK Voice Connector インフラストラクチャに送信されたバイト数。 単位: カウント

メトリクス	説明
CustomerToVcPacketsLost	顧客から Amazon Chime SDK Voice Connector インフラストラクチャへの転送中に失われたパケットの数。値は、呼び出しが終了するまで 1 分ごとに送信されます。値の数は累積です。 単位: カウント
CustomerToVcJitter	顧客から Amazon Chime SDK Voice Connector インフラストラクチャに送信されたパケットの平均ジッター。 単位: マイクロ秒
VcToCustomerRtpPackets	Amazon Chime SDK Voice Connector インフラストラクチャからカスタマーに送信された RTP パケットの数。 単位: カウント
VcToCustomerRtpBytes	Amazon Chime SDK Voice Connector インフラストラクチャから RTP パケットで顧客に送信されたバイト数。 単位: カウント
VcToCustomerRtcpPackets	Amazon Chime SDK Voice Connector インフラストラクチャからカスタマーに送信された RTCP パケットの数。 単位: カウント
VcToCustomerRtcpBytes	Amazon Chime SDK Voice Connector インフラストラクチャから RTCP パケットで顧客に送信されたバイト数。 単位: カウント

メトリクス	説明
VcToCustomerPacketsLost	Amazon Chime SDK Voice Connector インフラストラクチャからお客様への転送中に失われたパケットの数。値は、呼び出しが終了するまで 1 分ごとに送信されます。値の数は累積です。 単位: カウント
VcToCustomerJitter	Amazon Chime SDK Voice Connector インフラストラクチャから顧客に送信されたパケットの平均ジッター。 単位: マイクロ秒
RTTBetweenVcAndCustomer	顧客と Amazon Chime SDK Voice Connector インフラストラクチャ間の平均往復時間。 単位: マイクロ秒
MOSBetweenVcAndCustomer	顧客と Amazon Chime SDK Voice Connector インフラストラクチャ間の音声ストリームに関連する推定平均オプショナルスコア (MOS)。 単位: 1.0 ~ 4.4 のスコア。スコアが高いほど、認識されるオーディオ品質が向上します。
RemoteToVcRtpPackets	リモートエンドから Amazon Chime SDK Voice Connector インフラストラクチャに送信された RTP パケットの数。 単位: カウント
RemoteToVcRtpBytes	リモートエンドから RTP パケットの Amazon Chime SDK Voice Connector インフラストラクチャに送信されたバイト数。 単位: カウント

メトリクス	説明
RemoteToVcRtcpPackets	リモートエンドから Amazon Chime SDK Voice Connector インフラストラクチャに送信された RTCP パケットの数。 単位: カウント
RemoteToVcRtcpBytes	リモートエンドから RTCP パケットの Amazon Chime SDK Voice Connector インフラストラクチャに送信されたバイト数。 単位: カウント
RemoteToVcPacketsLost	リモートエンドから Amazon Chime SDK Voice Connector インフラストラクチャへの転送中に失われたパケットの数。値は、呼び出しが終了するまで 1 分ごとに送信されます。値の数は累積です。 単位: カウント
RemoteToVcJitter	リモートエンドから Amazon Chime SDK Voice Connector インフラストラクチャに送信されたパケットの平均ジッター。 単位: マイクロ秒
VcToRemoteRtpPackets	Amazon Chime SDK Voice Connector インフラストラクチャからリモートエンドに送信された RTP パケットの数。 単位: カウント
VcToRemoteRtpBytes	Amazon Chime SDK Voice Connector インフラストラクチャから RTP パケットでリモートエンドに送信されたバイト数。 単位: カウント

メトリクス	説明
VcToRemoteRtcpPackets	Amazon Chime SDK Voice Connector インフラストラクチャからリモートエンドに送信された RTCP パケットの数。 単位: カウント
VcToRemoteRtcpBytes	Amazon Chime SDK Voice Connector インフラストラクチャから RTCP パケットでリモートエンドに送信されたバイト数。 単位: カウント
VcToRemotePacketsLost	Amazon Chime SDK Voice Connector インフラストラクチャからリモートエンドへの転送中に失われたパケットの数。値は、呼び出しが終了するまで 1 分ごとに送信されます。値の数は累積です。 単位: カウント
VcToRemoteJitter	Amazon Chime SDK Voice Connector インフラストラクチャからリモートエンドに送信されたパケットの平均ジッター。 単位: マイクロ秒
RTTBetweenVcAndRemote	リモートエンドと Amazon Chime SDK Voice Connector インフラストラクチャ間の平均往復時間。 単位: マイクロ秒

メトリクス	説明
MOSBetweenVcAndRemote	リモートエンドと Amazon Chime SDK Voice Connector インフラストラクチャ間の音声ストリームに関連付けられた推定平均オプショナルスコア (MOS)。 単位: 単位: 1.0 ~ 4.4 のスコア。スコアが高いほど、認識されるオーディオ品質が向上します。

CloudWatch Amazon Chime SDK の ディメンション

Amazon Chime SDK で使用できる CloudWatch ディメンションは次のとおりです。

ディメンション	説明
VoiceConnectorId	メトリクスを表示する Amazon Chime SDK Voice Connector の識別子。
Region	イベントに関連付けられた AWS リージョン。

CloudWatch Amazon Chime SDK の ログ

CloudWatch ログにメトリクスを送信するように Amazon Chime SDK Voice Connector を設定できます。これを行うと、それらの Voice Connector のメディア品質メトリクスログを受信することもできます。

Amazon Chime SDK は、1 分に 1 回詳細なメトリクスを送信します。Amazon Chime SDK は、設定した Voice Connector で行われたすべての通話に対してそれらを送信し、ユーザーに代わって作成した CloudWatch Logs ロググループに送信します。

ロググループ名は、 の形式を使用します/aws/ChimeVoiceConnectorLogs/${*VoiceConnectorID*}。

メトリクスを送信するように Voice Connector を設定する方法の詳細については、「」を参照してくださいAmazon Chime SDK Voice Connector 設定の編集。

> **Note**
>
> パケット損失メトリクスは、 呼び出し中に蓄積されます。例えば、パケット損失が 11:01 に発生した場合、その損失値は呼び出しの残り分間保持されます。呼び出しの最後に、パケット損失メトリクスが 1 つ表示されます。

Amazon Chime SDK のログには、JSON 形式の以下のフィールドが含まれています。

フィールド	説明
voice_connector_id	通話を実行する Amazon Chime SDK Voice Connector ID。
event_timestamp	メトリクスが出力された時刻 (ミリ秒単位)。UNIX エポック (1970 年 1 月 1 日の午前 0 時) からの経過時間 (UTC) で表示されます。
call_id	トランザクション ID に対応します。
from_sip_user	呼び出しの開始ユーザー。
from_country	呼び出しの発信国。
to_sip_user	呼び出しの受信ユーザー。
to_country	呼び出しの受信国。
endpoint_id	呼び出しのもう一方のエンドポイントを示す不透明な識別子。 CloudWatch Logs Insights で を使用します。詳細については、「Amazon Logs ユーザーガイド」の CloudWatch「Logs Insights を使用したログデータの分析」を参照してください。 CloudWatch
aws_region	呼び出しの AWS リージョン。

フィールド	説明
cust2vc_rtp_packets	カスタマーから Amazon Chime SDK Voice Connector インフラストラクチャに送信された RTP パケットの数。
cust2vc_rtp_bytes	RTP パケットで顧客から Amazon Chime SDK Voice Connector インフラストラクチャに送信されたバイト数。
cust2vc_rtcp_packets	顧客から Amazon Chime SDK Voice Connector インフラストラクチャに送信された RTCP パケットの数。
cust2vc_rtcp_bytes	RTCP パケットで顧客から Amazon Chime SDK Voice Connector インフラストラクチャに送信されたバイト数。
cust2vc_packets_lost	顧客から Amazon Chime SDK Voice Connector インフラストラクチャへの転送中に失われたパケットの数。値は、呼び出しが終了するまで 1 分ごとに送信されます。値の数は累積です。
cust2vc_jitter	顧客から Amazon Chime SDK Voice Connector インフラストラクチャに送信されたパケットの平均ジッター。
vc2cust_rtp_packets	Amazon Chime SDK Voice Connector インフラストラクチャからカスタマーに送信された RTP パケットの数。
vc2cust_rtp_bytes	Amazon Chime SDK Voice Connector インフラストラクチャから RTP パケットで顧客に送信されたバイト数。
vc2cust_rtcp_packets	Amazon Chime SDK Voice Connector インフラストラクチャからカスタマーに送信された RTCP パケットの数。

フィールド	説明
vc2cust_rtcp_bytes	Amazon Chime SDK Voice Connector インフラストラクチャから RTCP パケットで顧客に送信されたバイト数。
vc2cust_packets_lost	Amazon Chime SDK Voice Connector インフラストラクチャからお客様への転送中に失われたパケットの数。値は、呼び出しが終了するまで 1 分ごとに送信されます。値の数は累積です。
vc2cust_jitter	Amazon Chime SDK Voice Connector インフラストラクチャから顧客に送信されたパケットの平均ジッター。
rtt_btwn_vc_and_cust	顧客と Amazon Chime SDK Voice Connector インフラストラクチャ間の平均往復時間。
mos_btwn_vc_and_cust	顧客と Amazon Chime SDK Voice Connector インフラストラクチャ間の音声ストリームに関連する推定平均オプショナルスコア (MOS)。
rem2vc_rtp_packets	リモートエンドから Amazon Chime SDK Voice Connector インフラストラクチャに送信された RTP パケットの数。
rem2vc_rtp_bytes	リモートエンドから RTP パケットの Amazon Chime SDK Voice Connector インフラストラクチャに送信されたバイト数。
rem2vc_rtcp_packets	リモートエンドから Amazon Chime SDK Voice Connector インフラストラクチャに送信された RTCP パケットの数。
rem2vc_rtcp_bytes	リモートエンドから RTCP パケットの Amazon Chime SDK Voice Connector インフラストラクチャに送信されたバイト数。

フィールド	説明
rem2vc_packets_lost	リモートエンドから Amazon Chime SDK Voice Connector インフラストラクチャへの転送中に失われたパケットの数。値は、呼び出しが終了するまで 1 分ごとに送信されます。値の数は累積です。
rem2vc_jitter	リモートエンドから Amazon Chime SDK Voice Connector インフラストラクチャに送信されたパケットの平均ジッター。
vc2rem_rtp_packets	Amazon Chime SDK Voice Connector インフラストラクチャからリモートエンドに送信された RTP パケットの数。
vc2rem_rtp_bytes	Amazon Chime SDK Voice Connector インフラストラクチャから RTP パケットでリモートエンドに送信されたバイト数。
vc2rem_rtcp_packets	Amazon Chime SDK Voice Connector インフラストラクチャからリモートエンドに送信された RTCP パケットの数。
vc2rem_rtcp_bytes	Amazon Chime SDK Voice Connector インフラストラクチャから RTCP パケットでリモートエンドに送信されたバイト数。
vc2rem_packets_lost	Amazon Chime SDK Voice Connector インフラストラクチャからリモートエンドへの転送中に失われたパケットの数。値は、呼び出しが終了するまで 1 分ごとに送信されます。値の数は累積です。
vc2rem_jitter	Amazon Chime SDK Voice Connector インフラストラクチャからリモートエンドに送信されたパケットの平均ジッター。

フィールド	説明
rtt_btwn_vc_and_rem	リモートエンドと Amazon Chime SDK Voice Connector インフラストラクチャ間の平均往復時間。
mos_btwn_vc_and_rem	リモートエンドと Amazon Chime SDK Voice Connector インフラストラクチャ間の音声ストリームに関連付けられた推定平均オプショナルスコア (MOS)。

SIP メッセージログ

Amazon Chime SDK Voice Connector の SIP メッセージログを受信するように選択できます。これを行うと、Amazon Chime SDK はインバウンドおよびアウトバウンドの SIP メッセージをキャプチャし、作成された CloudWatch Logs ロググループに送信します。ロググループ名は `/aws/ChimeVoiceConnectorSipMessages/${VoiceConnectorID}` です。以下のフィールドが JSON 形式でログに含まれます。

フィールド	説明
voice_connector_id	Amazon Chime SDK Voice Connector ID。
aws_region	イベントに関連付けられた AWS リージョン。
event_timestamp	メッセージがキャプチャされた時刻 (ミリ秒単位)。UNIX エポック (1970 年 1 月 1 日の午前 0 時) からの経過時間 (UTC) で表示されます。
call_id	Amazon Chime SDK Voice Connector 通話 ID。
sip_message	キャプチャされた完全な SIP メッセージ。

を使用した Amazon Chime SDK の自動化 EventBridge

Amazon EventBridge では、AWSサービスを自動化し、アプリケーションの可用性の問題やリソースの変更などのシステムイベントに自動的に対応できます。会議イベントの詳細については、「Amazon Chime SDK デベロッパーガイド」の「会議イベント」を参照してください。

Amazon Chime SDK がイベントを生成すると、ベストエフォート型の配信 EventBridge のためにイベントが に送信されます。つまり、Amazon Chime SDK はすべてのイベントを に送信しようとしますが EventBridge、まれにイベントが配信されない場合があります。詳細については、「Amazon ユーザーガイド」の「 AWSのサービスからのイベント」を参照してください。 EventBridge

> **Note**
>
> データを暗号化する必要がある場合、Amazon S3 マネージドキーを使用する必要があります。AWS Key Management Service に保存されているカスタマーマスターキーを使用したサーバー側の暗号化はサポートされていません。

を使用した Amazon Chime SDK Voice Connector の自動化 EventBridge

Amazon Chime SDK Voice Connector で自動的にトリガーできるアクションには、次のものがあります。

- AWS Lambda 関数の呼び出し
- Amazon Elastic Container Service タスクの起動
- Amazon Kinesis Video Streams へのイベントの中継
- AWS Step Functions ステートマシンのアクティブ化
- Amazon SNS トピックまたは Amazon SQS キューの通知

Amazon Chime SDK Voice Connector EventBridge で を使用する例には、次のようなものがあります。

- 通話終了後に通話の音声をダウンロードする Lambda 関数を有効にします。
- 通話の開始後に Amazon ECS タスクを起動してリアルタイム文字起こしを可能にする。

詳細については、「Amazon EventBridge ユーザーガイド」を参照してください。

Amazon Chime SDK Voice Connector ストリーミングイベント

Amazon Chime SDK Voice Connector は、このセクションで説明するイベントが発生した EventBridge ときに、 へのイベントの送信をサポートします。

Amazon Chime SDK Voice Connector ストリーミングの開始

Amazon Chime SDK Voice Connector は、Kinesis Video Streams へのメディアストリーミングが開始されたときに、このイベントを送信します。

Example イベントデータ

以下はこのイベントのサンプルデータです。

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-111122223333",
    "detail-type": "Chime VoiceConnector Streaming Status",
    "source": "aws.chime",
    "account": "111122223333",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "callId": "1112-2222-4333",
        "direction": "Outbound",
        "fromNumber": "+12065550100",
        "inviteHeaders": {
            "from": "\"John\" <sip:+12065550100@10.24.34.0>;tag=abcdefg",
            "to":
 "<sip:+13605550199@abcdef1ghij2klmno3pqr4M.voiceconnector.chime.aws:5060>",
            "call-id": "1112-2222-4333",
            "cseq": "101 INVITE",
            "contact": "<sip:user@10.24.34.0:6090>;",
            "content-type": "application/sdp",
            "content-length": "246"
        },
        "isCaller": false,
        "mediaType": "audio/L16",
        "sdp": {
            "mediaIndex": 0,
            "mediaLabel": "1"
        },
```

```
        "siprecMetadata": "<&xml version=\"1.0\" encoding=\"UTF-8\"&>;\r\n<recording
 xmlns='urn:ietf:params:xml:ns:recording:1'>",
        "startFragmentNumber": "1234567899444",
        "startTime": "yyyy-mm-ddThh:mm:ssZ",
        "streamArn": "arn:aws:kinesisvideo:us-east-1:123456M:stream/
ChimeVoiceConnector-abcdef1ghij2klmno3pqr4-111aaa-22bb-33cc-44dd-111222/111122223333",
        "toNumber": "+13605550199",
        "transactionId": "12345678-1234-1234",
        "voiceConnectorId": "abcdef1ghij2klmno3pqr4",
        "streamingStatus": "STARTED",
        "version": "0"
    }
}
```

Amazon Chime SDK Voice Connector ストリーミング終了

Amazon Chime SDK Voice Connector は、Kinesis Video Streams へのメディアストリーミングが終了したときに、このイベントを送信します。

Example イベントデータ

以下はこのイベントのサンプルデータです。

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-111122223333",
    "detail-type": "Chime VoiceConnector Streaming Status",
    "source": "aws.chime",
    "account": "111122223333",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "streamingStatus": "ENDED",
        "voiceConnectorId": "abcdef1ghij2klmno3pqr4",
        "transactionId": "12345678-1234-1234",
        "callId": "1112-2222-4333",
        "direction": "Inbound",
        "fromNumber": "+12065550100",
        "inviteHeaders": {
            "from": "\"John\" <sip:+12065550100@10.24.34.0>;tag=abcdefg",
            "to": "<sip:
+13605550199@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws:5060>",
            "call-id": "1112-2222-4333",
```

```
            "cseq": "101 INVITE",
            "contact": "<sip:user@10.24.34.0:6090>",
            "content-type": "application/sdp",
            "content-length": "246"
        },
        "isCaller": false,
        "mediaType": "audio/L16",
        "sdp": {
            "mediaIndex": 0,
            "mediaLabel": "1"
        },
        "siprecMetadata": "<&xml version=\"1.0\" encoding=\"UTF-8\"&>\r\n<recording
 xmlns='urn:ietf:params:xml:ns:recording:1'>",
        "startFragmentNumber": "1234567899444",
        "startTime": "yyyy-mm-ddThh:mm:ssZ",
        "endTime": "yyyy-mm-ddThh:mm:ssZ",
        "streamArn": "arn:aws:kinesisvideo:us-east-1:123456:stream/
ChimeVoiceConnector-abcdef1ghij2klmno3pqr4-111aaa-22bb-33cc-44dd-111222/111122223333",
        "toNumber": "+13605550199",
        "version": "0"
    }
}
```

Amazon Chime SDK Voice Connector ストリーミングの更新

Amazon Chime SDK Voice Connector は、Kinesis Video Streams へのメディアストリーミングが更新されると、このイベントを送信します。

Example イベントデータ

以下はこのイベントのサンプルデータです。

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-111122223333",
    "detail-type": "Chime VoiceConnector Streaming Status",
    "source": "aws.chime",
    "account": "111122223333",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "callId": "1112-2222-4333",
        "updateHeaders": {
```

```
            "from": "\"John\" <sip:+12065550100@10.24.34.0>;;tag=abcdefg",
            "to": "<sip:
+13605550199@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws:5060>",
            "call-id": "1112-2222-4333",
            "cseq": "101 INVITE",
            "contact": "<sip:user@10.24.34.0:6090>",
            "content-type": "application/sdp",
            "content-length": "246"
        },
        "siprecMetadata": "<&xml version=\"1.0\" encoding=\"UTF-8\"&>\r\n<recording
 xmlns='urn:ietf:params:xml:ns:recording:1'>",
        "streamingStatus": "UPDATED",
        "transactionId": "12345678-1234-1234",
        "version": "0",
        "voiceConnectorId": "abcdef1ghij2klmno3pqr4"
    }
}
```

Amazon Chime SDK Voice Connector ストリーミングが失敗する

Amazon Chime SDK Voice Connector は、Kinesis Video Streams へのメディアストリーミングが失敗した場合に、このイベントを送信します。

Example イベントデータ

以下はこのイベントのサンプルデータです。

```
{
  "version": "0",
  "id": "12345678-1234-1234-1234-111122223333",
  "detail-type": "Chime VoiceConnector Streaming Status",
  "source": "aws.chime",
  "account": "111122223333",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [],
  "detail": {
       "streamingStatus":"FAILED",
       "voiceConnectorId":"abcdefghi",
       "transactionId":"12345678-1234-1234",
       "callId":"1112-2222-4333",
       "direction":"Inbound",
       "failTime":"yyyy-mm-ddThh:mm:ssZ",
       "failureReason": "Internal failure",
```

```
        "version":"0"
    }
}
```

を使用した API コールAWS CloudTrailのログ記録

Amazon Chime SDK は、ユーザーAWS CloudTrail、ロール、または service によって Amazon Chime SDK で実行されたアクションを記録するAWSサービスである と統合されています。 は、Amazon Chime SDK コンソールからの呼び出しや Amazon Chime SDK API へのコード呼び出しを含む、Amazon Chime SDK のすべての API コールをイベントとして CloudTrail キャプチャします。 APIs

証跡を作成する場合は、Amazon Chime SDK の CloudTrailイベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます。 Amazon S3 証跡を設定しない場合でも、イベント履歴ページの CloudTrail コンソールで最新のイベントを表示できます。 情報には、各リクエスト、リクエスト元の IP アドレス、リクエスト者が含まれます。

CloudTrail AWSアカウントを作成すると、 がアカウントで有効になります。Amazon Chime 管理コンソールが API コールを行うと、 はそのアクティビティをイベント CloudTrail に記録します。イベントを表示するには、 CloudTrail コンソールを起動し、イベント履歴 に移動します。AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、「イベント履歴 を使用した CloudTrail イベントの表示」を参照してください。

の詳細については CloudTrail、「 AWS CloudTrailユーザーガイド」を参照してください。

証跡の作成

以下のトピックでは、 CloudTrail コンソールを使用して証跡を作成する方法について説明します。デフォルトでは、コンソールで証跡を作成すると、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。

これらのトピックは、リストされている順序で実行してください。

1. 「証跡作成の概要」
2. CloudTrail でサポートされているサービスと統合
3. の Amazon SNS 通知の設定 CloudTrail
4. 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからの CloudTrail ログファイルの受信

証跡によってキャプチャされたデータ

CloudTrail は、すべての Amazon Chime SDK アクションを記録します。アクションの詳細については、「Amazon Chime SDK API リファレンス」を参照してください。例えば、、 アクションを呼び出すとCreateAccount、 CloudTrail ログファイルにエントリが生成されます。すべてのイベントには、リクエストを生成したユーザーに関する情報が含まれています。このアイデンティティ情報は以下のことを判断するのに役立ちます：

- リクエストが、ルートと IAM ユーザー認証情報のどちらを使用して送信されたか。
- 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一時的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 サービスによって送信されたかどうか。

詳細については、「CloudTrail userIdentity 要素」を参照してください。

Amazon Chime SDK ログファイルエントリについて

証跡は、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できるようにする設定です。 CloudTrail ログファイルには、1 つ以上のログエントリが含まれます。イベントはあらゆるソース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、リクエストのパラメータなどの情報が含まれます。 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。

Amazon Chime SDK のエントリは、chime.amazonaws.com イベントソースによって識別されます。

Amazon Chime SDK アカウントに Active Directory を設定している場合は、「 を使用した AWS Directory Service API コールのログ記録 CloudTrail」を参照してください。ここでは、Amazon Chime SDK ユーザーのサインイン能力に影響する可能性のある問題をモニタリングする方法について説明します。

次の例は、Amazon Chime SDK の CloudTrail ログエントリを示しています。

```
{"eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AAAAAABBBBBBBBEXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice",
            "accountId":"0123456789012",
```

```
            "accessKeyId":"AAAAAABBBBBBBBEXAMPLE",
            "sessionContext":{
               "attributes":{
                  "mfaAuthenticated":"false",
                  "creationDate":"2017-07-24T17:57:43Z"
               },
               "sessionIssuer":{
                  "type":"Role",
                  "principalId":"AAAAAABBBBBBBBEXAMPLE",
                  "arn":"arn:aws:iam::123456789012:role/Joe",
                  "accountId":"123456789012",
                  "userName":"Joe"
               }
            }
         } ,
         "eventTime":"2017-07-24T17:58:21Z",
         "eventSource":"chime.amazonaws.com",
         "eventName":"AddDomain",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"72.21.198.64",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36",
         "errorCode":"ConflictException",
         "errorMessage":"Request could not be completed due to a conflict",
         "requestParameters":{
            "domainName":"example.com",
            "accountId":"11aaaaaa1-1a11-1111-1a11-aaadd0a0aa00"
         },
         "responseElements":null,
         "requestID":"be1bee1d-1111-11e1-1eD1-0dc1111f1ac1",
         "eventID":"00fbeee1-123e-111e-93e3-11111bfbfcc1",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
```


Amazon Chime SDK のコンプライアンス検証

サードパーティー監査人は、SOC、PCI、FedRAMP、および HIPAA など複数の AWS コンプライアンスプログラムの一環として、AWS のサービスのセキュリティとコンプライアンスを評価します。

AWS のサービス が特定のコンプライアンスプログラムの範囲内に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別の範囲」の「AWS のサービス」と「」の「AWS のサービス」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、サードパーティー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、「Downloading Reports in AWS Artifact」を参照してください。

AWS のサービスを使用する際のユーザーのコンプライアンス責任は、ユーザーのデータの機密性や貴社のコンプライアンス目的、適用される法律および規制によって決まります。AWS では、コンプライアンスに役立つ次のリソースを提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド - これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境を AWS にデプロイするための手順を示します。
- 「Amazon Web Services での HIPAA のセキュリティとコンプライアンスのためのアーキテクチャ」 - このホワイトペーパーは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法を説明しています。

  > **Note**
  >
  > すべての AWS のサービスが HIPAA 適格であるわけではありません。詳細については、「HIPAA 対応サービスのリファレンス」を参照してください。

- AWS コンプライアンスのリソース - このワークブックおよびガイドのコレクションは、顧客の業界と拠点に適用されるものである場合があります。
- AWS Customer Compliance Guide — コンプライアンスの観点から見た責任共有モデルを理解できます。このガイドは、AWS のサービスを保護するためのベストプラクティスを要約したものであり、複数のフレームワーク (米国標準技術研究所 (NIST)、ペイメントカード業界セキュリティ標準評議会 (PCI)、国際標準化機構 (ISO) など) にわたるセキュリティ統制へのガイダンスがまとめられています。
- 「AWS Config デベロッパーガイド」の「ルールでのリソースの評価」 - AWS Config サービスは、自社のプラクティス、業界ガイドライン、および規制に対するリソースの設定の準拠状態を評価します。
- AWS Security Hub - この AWS のサービスは、AWS 内のセキュリティ状態の包括的なビューを提供します。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、「Security Hub のコントロールリファレンス」を参照してください。

- AWS Audit Manager - この AWS のサービスは、AWS の使用状況を継続的に監査して、リスクの管理方法や、規制および業界標準へのコンプライアンスの管理方法を簡素化するために役立ちます。

Amazon Chime SDK の耐障害性

AWS のグローバルインフラストラクチャは、AWS リージョンとアベイラビリティーゾーンを中心として構築されています。AWSリージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立および隔離されたアベイラビリティーゾーンがあります。アベイラビリティーゾーンでは、ゾーン間で中断することなく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よりも可用性、耐障害性、および拡張性が優れています。

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。

Amazon Chime SDK は、 AWS グローバルインフラストラクチャに加えて、データの耐障害性とバックアップのニーズに対応できるようにさまざまな機能を提供します。詳細については、Amazon Chime SDK Voice Connector グループの管理およびAmazon Chime SDK Voice Connector メディアを Kinesis にストリーミングするを参照してください。

Amazon Chime SDK のインフラストラクチャセキュリティ

これはマネージドサービスであり、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 フレームワーク」の「インフラストラクチャ保護」を参照してください。

AWS 公開版 API コールを使用して、ネットワーク経由でアクセスします。クライアントは以下をサポートする必要があります:

- Transport Layer Security (TLS)。TLS 1.2 が必須です。TLS 1.3 が推奨されます。
- 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。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 ServiceAWS 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。

開始

以下のトピックでは、Amazon Chime SDK が提供する管理タスクを開始する方法について説明します。

トピック

Amazon Chime SDK アカウントの電話番号の設定

Amazon Chime SDK 管理アカウントでは、次の電話オプションを使用できます。

Amazon Chime SDK Voice Connector

既存の電話システムにセッション開始プロトコル (SIP) トランキングサービスを提供します。Amazon Chime SDK コンソールで既存の電話番号を移行するか、新しい電話番号をプロビジョニングします。これには緊急番号が含まれます。詳細については、Amazon Chime SDK Voice Connector の管理 および 緊急通報の設定 を参照してください。

Amazon Chime SDK SIP メディアアプリケーション

Amazon Chime SDK SIP メディアアプリケーションを使用すると、通常はプライベートブランチ電話交換 (PBX) に基づいて構築するカスタムシグナリングとメディア命令を簡単かつ迅速に作成できます。詳細については、SIP メディアアプリケーションの管理 を参照してください。

Amazon Chime SDK での電話番号の管理

このセクションのトピックでは、Amazon Chime SDK で使用する電話番号を管理する方法について説明します。

番号は以下の方法で取得できます。

- Amazon Chime SDK が提供する番号プールから順番に番号をプロビジョニングします。これは身元確認の要件がない国でのみ可能です。
- 既存の番号を別のキャリアから Amazon Chime SDK に移植します。
- 国際電話番号を注文する。

プロビジョニングとポーティングのプロセスにより、番号がインベントリに追加されます。次に、その番号を Amazon Chime SDK 音声コネクタ、Amazon Chime SDK 音声コネクタグループ、または Amazon Chime SDK SIP メディアアプリケーションで使用します。

> **Note**
>
> フリーダイヤル番号を移植して、Amazon Chime SDK 音声コネクタや Amazon Chime SIP メディアアプリケーションで使用できます。Amazon Chime Business Calling は通話料無料の番号をサポートしていません。詳細については、このガイドで後述する「既存の電話番号の移植」を参照してください。

Amazon Chime SDK 音声コネクタグループまたは Amazon Chime SDK 音声コネクタグループで電話番号を使用するには、Amazon Chime SDK コンソールを使用して番号を割り当てます。音声コネクタの詳細については、を参照してください。Amazon Chime SDK Voice Connector の管理Voice Connector に番号を割り当てる方法については、を参照してください音声コネクタまたは音声コネクタグループへの番号の割り当て。

> **Note**
>
> また、音声コネクタを使用して Amazon Chime からの緊急通報を有効にします。ただし、Amazon Chime SDK は米国外では緊急通報サービスを提供していません。Amazon Chime SDK が米国向けに提供する緊急通報サービスを変更するには、サードパーティの緊急サービスプロバイダーから緊急通報ルーティング番号を取得し、その番号を Amazon Chime

SDK に渡し、その番号を Amazon Chime SDK 音声コネクタに割り当てます。詳細については、「サードパーティー緊急ルーティング番号の設定」を参照してください。

SIP メディアアプリケーションで電話番号を使用するには、その電話番号をアプリケーションに関連付けられた SIP ルールに追加します。SIP メディアアプリケーションの詳細については、を参照してくださいSIP メディアアプリケーションの使用。SIP ルールに電話番号を追加する方法の詳細については、を参照してくださいSIP ルールの作成。

> **Note**
>
> Amazon Chime SDK 音声コネクタと Amazon Chime SDK SIP メディアアプリケーションには帯域幅要件があります。詳細については、「帯域幅の要件」を参照してください。

コンテンツ

電話番号のプロビジョニング

Amazon Chime SDK コンソールを使用して、Amazon Chime SDK アカウントの電話番号をプロビジョニングします。以下のアプローチのいずれかを選択できます。

- Amazon Chime SDK 音声コネクタ — 既存の電話システムと統合できます。詳細については、「Amazon Chime SDK Voice Connector の管理」を参照してください。
- Amazon Chime SDK SIP メディアアプリケーション — Amazon Chime SDK ミーティングや Amazon Lex などのインタラクティブな音声応答サービスと統合できます。詳細については、「SIP メディアアプリケーションの管理」を参照してください。

Amazon Chime SDK によって提供される番号プールから電話番号をプロビジョニングします。プロビジョニングが完了すると、電話番号がインベントリに表示され、個々のユーザーに割り当てることができます。

> **Important**
>
> 本人確認の要件がない国の場合にのみ、この手順に従ってください。識別要件のある国の電話番号のプロビジョニングについては、「国際電話番号のリクエスト」を参照してください。

電話番号をプロビジョニングするには

1. https://console.aws.amazon.com/chime-sdk/home にある Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [電話番号] で、[電話番号管理] を選択します。
3. [注文] タブを選択し、[電話番号の提供] を選択します。
4. 「電話番号のプロビジョニング」ダイアログボックスで、「Voice Connector」または「SIP メディアアプリケーションダイヤルイン」を選択し、「次へ」を選択します。

   > **Note**
   >
   > 電話番号に割り当てられた製品タイプは、請求に影響します。デフォルトの通話名を設定すると、システムはそれを米国内で新しく設定した電話番号に割り当てます。また、SIP メディアアプリケーションのアウトバウンドコールでは、発信者 ID がインベントリ内の番号と一致する必要があります。または、関連する Lambda 関数によって送り返されたインバウンドコールの元の発信者 ID と一致する必要があります。たとえば、この関数はアクションを使用できます。`CallAndBridge`詳細については、このガイドと CallAndBridgeAmazon Chime SDK 開発者ガイドのを参照してくださいアウトバウンドコール名を設定する。

5. 「電話番号のプロビジョニング」ページで、次の操作を行います。
   - 「アプリケーションタイプの選択」 リストを開き、「音声コネクタ」または「SIP メディアアプリケーションダイヤルイン」のいずれかのオプションを選択します。

     選択内容は、ステップ 6 で表示される国に影響します。

- (オプション) [電話番号の詳細] の [名前] ボックスに、コストセンターやオフィスの場所など、電話番号のわかりやすい名前を入力します。

  このフィールドは、アウトバウンドコール名とは異なります。アウトバウンドコール名の詳細については、アウトバウンドコール名を設定する本ガイドのを参照してください。

6. 「番号検索」で「国」リストを開いて国を選択し、次のいずれかを実行します。

   - 米国外の電話番号の場合:

     a. 「タイプ」リストを開き、オプションを選択します。

        選択した国によっては、どのタイプも使用できない場合があります。たとえば、カナダでは市内番号、イタリアではフリーダイヤル番号しか選択できません。

     b. [検索] ボタンを選択します。

   - 米国の電話番号の場合:

     a. 「タイプ」リストを開き、オプションを選択します。

     b. 「エリア」リストを開き、「ロケーション」または「エリアコード」を選択します。

        - 「場所」を選択した場合は、「州」リストを開いて州を選択し、次に都市を入力して「検索」ボタンを選択します。

          > **Note**
          > 検索しても数字が返されない場合は、「市区町村」フィールドをクリアして、もう一度検索してください。

        - [エリアコード] を選択した場合は、[エリアコード] ボックスにエリアコードを入力し、[検索] ボタンを選択します。

7. 表示されるリストから 1 つまたは複数の電話番号を選択します。
8. (オプション) [電話番号の詳細] に、1 つまたは複数の番号の名前を入力します。前の手順で複数の番号を選択した場合、その名前はすべての番号に適用されます。
9. 「電話番号注文を作成」を選択します。

プロビジョニングが行われている間、電話番号は「注文」タブと「保留中」タブに表示されます。プロビジョニングが完了すると、その番号が「インベントリ」タブに表示されます。

国際電話番号のリクエスト

このセクションのステップでは、Amazon Chime SDK で使用する国際電話番号をリクエストする方法について説明します。国際電話番号は SIP メディアアプリケーションダイヤルイン製品タイプでのみ使用できます。

多くの国では規制上、国際番号を購入するにあたって以下が必要です。

- ローカルアドレス
- Amazon Chime SDK または当社の通信事業者が発行するお客様の身元を証明する書類

Amazon Chime SDK がリクエストに対応するまでには 2 ~ 6 週間かかります。各国の書類要件の詳細については、「the section called “国別電話番号要件”」を参照してください。

識別要件のある国で国際電話番号をリクエストするには

1. 次のいずれかを行います。
   - Amazon Chime SDK コンソールを開き、ナビゲーションペインの [お問い合わせ] で [Support] を選択します。Support センターに移動します。「テクニカル」を選択します。
   - AWS Support をご利用の場合は、 AWS Support センターページを開き、必要に応じてサインインし、[ケースを作成]、[テクニカルサポート] の順に選択します。[Service] で、[Chime] を選択します。
2. [カテゴリ] で [その他] を選択します。
3. [Subject] (件名) について、[Provisioning international numbers] (国際番号のプロビジョニング) に番号を入力します。
4. [Issue または Description] (発行または説明) に以下を入力します。
   - 個人または法人
   - 氏名 (個人名または法人名)
   - 番号のタイプ (市内または通話料無料)
   - 国
   - 電話番号の数
5. 次のいずれかを行います。

- Amazon Chime SDK コンソールからサポートリクエストを送信する場合は、[メール] に Amazon Chime 管理者アカウントに関連付けられている E メールアドレスを入力し、[リクエストを送信] を選択します。
- AWS Support センターでケースを作成する場合は、[添付ファイル] で [ファイルを選択] を選択し、必要な書類を添付してください。[Contact options] で、連絡方法を選択します。必要に応じて、[Additional contacts] に、ケースのステータス更新を通知する先のユーザーの E メールアドレスを入力します。

AWS Support は、サポートリクエストに応答して、電話番号をプロビジョニングできるかどうかをユーザーに通知します。 AWS Support からの回答は、以下のいずれかの方法で受け取ります。

- Amazon Chime SDK コンソールからSupport リクエストを送信した場合、 AWS サポートは、 AWS アカウントの連絡先情報の [代替連絡先] で指定されている運用連絡先にメールを送信します。詳細については、『 AWS Billing and Cost Management ユーザーガイド』の「連絡先情報の編集」を参照してください。
- AWS Support Center でケースを作成した場合、選択した連絡方法および追加の連絡先として入力した E メールアドレスに基づいてレスポンスを受け取ります。

番号がプロビジョニングされると、Amazon Chime SDK コンソールで番号を表示できます。[電話番号] で [電話番号管理] を選択します。電話番号は「在庫」ページに表示されます。

6. SIP ルールを使用して、電話番号を適切な SIP メディアアプリケーションに割り当てます。

発信通話の制限

中国

中国の通信事業者は、中国への国際ルートをますますブロックしています。Amazon Chime SDK は引き続き既存のお客様をサポートしますが、中国への通話を承認されたすべてのお客様は、次の条件を満たす必要があります。

資格基準

サポートされていないユースケース

- 通話時間が短く、アラートが 15 秒未満。

- 大量の通話、特に同じアウトバウンド発信者 ID (1 分間に 5 回以上) を使用して短時間の通話。
- あらゆる形式の勧誘電話。
- 無効な電話番号へのあらゆる電話。宛先の電話番号はすべて正確であることが検証されていなければなりません。
- 同じ FROM 番号または TO 番号を使用して繰り返し呼び出し。
- 事前に承認されていない任意の番号から中国への電話を試みます。

サポートされているユースケース

- スイートや IT サポート機能など、既知の事業体に直接電話をかける。
- 住宅配置スキームや製品購入など、ビジネスとやり取りしようとするユーザーを呼び出す。

設定に必要なデータ

中国の電話番号 (+86) を呼び出すためのアクセス許可を取得するには、次の手順に従います。

- 中国への通話に使用される電話番号の完全かつ完全なリストを提供します。
  - 番号は、Amazon Chime SDK によって提供される DID である必要があります。他の番号は許容されません。
  - この番号は、香港、マカオ、台湾、中国、またはシンガポールが提供する DID であってはなりません。

> **Note**
>
> 上記のリストはいつでも変更される可能性があります。

- 電話番号ごとに、ビジネスの名前を識別する通知を記録する必要があります。これにより、電話番号を呼び出したすべてのユーザーが録音を聞き、どの企業が電話をかけているかを把握できます。
- 中国に電話をかけるためのユースケースの詳細な説明AWSを に提供し、このトピックで説明されている資格基準を満たしていることを確認する必要があります。

基準に違反した場合の影響

Amazon Chime SDK には、中国を呼び出すためのゼロトレランスポリシーがあります。上記の制限されたユースケースのいずれかでサービスを使用する場合、Amazon Chime SDK アカウントは停止されます。Amazon Chime SDK 管理者は、これらの制限も認識できるように、このポリシーを組織

の他のメンバーに伝える必要があります。ルールを無視することは、違反の理由としては許容されません。

サービス保証

中国の通信事業者が事前の警告なしに主要な国際ルートをブロックし、中国への電話機能に影響する場合は、Amazon Chime SDK サービスレベルアグリーメントの除外が適用されます。

国別電話番号要件

米国以外で電話番号を購入して使用するには、現地の住所や特定の身分証明書が必要になることがよくあります。住所には、勤務先または個人の住所を指定できます。次の表は識別が必要な国の一覧です。国際電話番号をリクエストする場合、または既存の電話番号を移行する場合、Amazon Chime SDK サポートは必要なドキュメントを送信するためにお客様と連携しています。

> **Note**
>
> 電話番号を使用するエンドユーザーの ID とアドレスを必ず入力してください。

トピック

- オーストラリア
- オーストリア
- カナダ
- デンマーク
- フィンランド
- ドイツ
- アイルランド
- イタリア
- ニュージーランド
- ナイジェリア
- プエルトリコ
- 韓国
- スウェーデン
- スイス

- 英国

オーストラリア

以下の表に示すのは、オーストラリアにおける電話番号の注文と移植の要件の一覧と説明です。

電話番号の注文

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
Amazon Chime SDK SDK SIP メディアアプリケーションのダイヤルイン	ローカル	はい	• 勤務先住所 • 所在地の証明 勤務先住所は、対応する電話番号と同じ地理的ゾーンでなければなりません。
	通話料無料	はい	• 勤務先住所 国際住所が許容されます。

電話番号の移植

サポートされる製品タイプ	番号タイプ	必須 ID
SIP メディアアプリケーションダイヤルイン	ローカル	• 現在のプロバイダーからの最終請求書 • 認証書
	通話料無料	• 現在のプロバイダーからの最終請求書 • 認証書

オーストリア

以下の表に示すのは、オーストリアにおける電話番号の注文と移植の要件の一覧と説明です。

電話番号の注文

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
SIP メディアアプリケーションダイヤルイン	ローカル	はい	• 勤務先住所 • 同じ局番内の別の電話番号を持つネットワークオペレータから発行された請求書などの通信接続サービスの証明。 - または - インターネットプロバイダーから発行されたインターネットアクセスに関する請求書で固定 IP アドレスが適切な地域にあるもの。 勤務先住所は、対応する電話番号と同じ地理的ゾーンでなければなりません。
	国内地域番号: +43 720	はい	• 勤務先住所

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
			住所は国内に存在する必要がある
	通話料無料	はい	• 勤務先住所 許容外部アドレス

電話番号の移植

サポートされる製品タイプ	番号タイプ	必須 ID
SIP メディアアプリケーションダイヤルイン	ローカル	• 現在のプロバイダーからの最終請求書 • 認証書
	通話料無料	• 現在のプロバイダーからの最終請求書 • 認証書

カナダ

以下の表に示すのは、カナダにおける電話番号の注文と移植の要件の一覧と説明です。

電話番号の注文

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
SIP メディアアプリケーションダイヤルイン	ローカル	いいえ	該当なし
通話料無料	いいえ	該当なし	該当なし

電話番号の移植

サポートされる製品タイプ	番号タイプ	必須 ID
SIP メディアアプリケーションダイヤルイン	ローカル	• 現在のプロバイダーからの最終請求書 • 認証書
	通話料無料	• 現在のプロバイダーからの最終請求書 • 認証書

デンマーク

以下の表に示すのは、デンマークにおける電話番号の注文と移植の要件の一覧と説明です。

電話番号の注文

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
SIP メディアアプリケーションダイヤルイン	ローカル	いいえ	該当なし
	通話料無料	いいえ	該当なし

電話番号の移植

サポートされる製品タイプ	番号タイプ	必須 ID
SIP メディアアプリケーションダイヤルイン	ローカル	• 現在のプロバイダーからの最終請求書 • 認証書
	通話料無料	• 現在のプロバイダーからの最終請求書 • 認証書

フィンランド

以下の表に示すのは、フィンランドにおける電話番号の注文と移植の要件の一覧と説明です。

電話番号の注文

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
SIP メディアアプリケーションダイヤルイン	ローカル	はい	• 勤務先住所 • 所在地の証明 勤務先住所は、対応する電話番号と同じ地理的リージョンでなければなりません。
	国内地域番号: +358 075	いいえ	該当なし
	通話料無料	いいえ	該当なし

電話番号の移植

サポートされる製品タイプ	番号タイプ	必須 ID
SIP メディアアプリケーションダイヤルイン	ローカル	• 現在のプロバイダーからの最終請求書 • 認証書
	通話料無料	• 現在のプロバイダーからの最終請求書 • 認証書

ドイツ

以下の表に示すのは、ドイツにおける電話番号の注文と移植の要件の一覧と説明です。

電話番号の注文

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
SIP メディアアプリケーションダイヤルイン	ローカル	はい	• 勤務先住所 • 事業者登録のコピー、または個人の場合は ID のコピー • 公共料金領収書などの住所証明 勤務先住所は、対応する電話番号と同じ地理的ゾーンでなければなりません。
	国内地域番号: +49 32	はい	• 勤務先住所 • 事業者登録のコピー、または個人の場合は ID のコピー • 公共料金領収書などの住所証明 住所は国内に存在する必要がある
	通話料無料	はい	• 勤務先住所 • 公共料金領収書などの住所証明

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
			住所は国内に存在する必要がある まず現地機関から番号を直接取得する必要があります。プロセスに関する詳細情報は、リクエストするときに提供されます。

電話番号の移植

サポートされる製品タイプ	番号タイプ	必須 ID
SIP メディアアプリケーションダイヤルイン	ローカル	• 現在のプロバイダーからの最終請求書 • 認証書 • 勤務先住所 • 事業者登録のコピー • 会社代表者 ID のコピー 勤務先住所は、対応する電話番号と同じ地理的ゾーンでなければなりません。
	通話料無料	• 現在のプロバイダーからの最終請求書 • 認証書 • NRA から入手した番号証明書

サポートされる製品タイプ	番号タイプ	必須 ID
		まず現地機関から番号を直接取得する必要があります。プロセスに関する詳細情報は、リクエストするときに提供されます。

アイルランド

以下の表に示すのは、アイルランドにおける電話番号の注文と移植の要件の一覧と説明です。

電話番号の注文

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
SIP メディアアプリケーションダイヤルイン	ローカル	はい	• 勤務先住所 勤務先住所は、対応する電話番号と同じ地理的リージョンでなければなりません。
	ユニバーサルアクセスと VOIP プレフィックス: +353 0818、+353 076	はい	• 勤務先住所 住所は国内に存在する必要がある
	通話料無料機能	いいえ	該当なし

電話番号の移植

サポートされる製品タイプ	番号タイプ	必須 ID
SIP メディアアプリケーションダイヤルイン	ローカル	• 現在のプロバイダーからの最終請求書 • 認証書
	通話料無料	• 現在のプロバイダーからの最終請求書 • 認証書

イタリア

以下の表に示すのは、イタリアにおける電話番号の注文と移植の要件の一覧と説明です。

電話番号の注文

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
SIP メディアアプリケーションダイヤルイン	ローカル	はい	• 勤務先住所 • 所在地の証明 • 事業者登録のコピー • パスポートまたはエンドユーザーの ID 勤務先住所は、対応する電話番号と同じ地理的リージョンでなければなりません。
	通話料無料機能	いいえ	該当なし

電話番号の移植

サポートされる製品タイプ	番号タイプ	必須 ID
SIP メディアアプリケーションダイヤルイン	ローカル	• 現在のプロバイダーからの最終請求書 • 認証書 • 会社代表者のパスポートまたは ID のコピー • 現地の事業者登録のコピー、または個人の住所証明
	通話料無料機能	• 現在のプロバイダーからの最終請求書 • 認証書

ニュージーランド

以下の表に示すのは、ニュージーランドにおける電話番号の注文と移植の要件の一覧と説明です。

電話番号の注文

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
SIP メディアアプリケーションダイヤルイン	ローカル	いいえ	該当なし
	通話料無料	いいえ	該当なし

電話番号の移植

サポートされる製品タイプ	番号タイプ	必須 ID
SIP メディアアプリケーションダイヤルイン	ローカル	サポートされません

サポートされる製品タイプ	番号タイプ	必須 ID
	通話料無料	• 現在のプロバイダーからの最終請求書 • 認証書

ナイジェリア

以下の表に示すのは、ナイジェリアにおける電話番号の注文の要件の一覧と説明です。

電話番号の注文

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
SIP メディアアプリケーションダイヤルイン	ローカル	はい	• 勤務先住所 外国の住所も使用可能。

プエルトリコ

以下の表に示すのは、プエルトリコにおける電話番号の注文と移植の要件の一覧と説明です。

電話番号の注文

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
Business Calling Amazon Chime SDK Voice Connector	ローカル	いいえ	該当なし
通話料無料	いいえ	該当なし	該当なし

韓国

以下の表に示すのは、韓国における電話番号の注文と要件の一覧と説明です。

電話番号の注文

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
SIP メディアアプリケーションダイヤルイン	通話料無料	はい	• 勤務先住所 • 所在地の証明 住所は国内に存在する必要がある

スウェーデン

以下の表に示すのは、スウェーデンにおける電話番号の注文と移植の要件の一覧と説明です。

電話番号の注文

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
SIP メディアアプリケーションダイヤルイン	ローカル	いいえ	該当なし
	通話料無料	いいえ	該当なし

電話番号の移植

サポートされる製品タイプ	番号タイプ	必須 ID
SIP メディアアプリケーションダイヤルイン	ローカル	• 現在のプロバイダーからの最終請求書 • 認証書

サポートされる製品タイプ	番号タイプ	必須 ID
	通話料無料	• 現在のプロバイダーからの最終請求書 • 認証書

スイス

以下の表に示すのは、スイスにおける電話番号の注文と移植の要件の一覧と説明です。

電話番号の注文

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
SIP メディアアプリケーションダイヤルイン	ローカル	はい	• 勤務先住所 • 所在地の証明 • 事業者登録のコピー、または個人の場合は ID のコピー 勤務先住所は、対応する電話番号と同じ地理的ゾーンでなければなりません。
	外線発信番号: +41 051、+41 058	はい	• 勤務先住所 住所は国内に存在する必要がある
	通話料無料	はい	• 勤務先住所 • 事業者登録のコピー、または個人

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
			の場合は ID のコピー 許容外部アドレス

電話番号の移植

サポートされる製品タイプ	番号タイプ	必須 ID
SIP メディアアプリケーションダイヤルイン	ローカル	• 現在のプロバイダーからの最終請求書 • 認証書 • 勤務先住所 許容外部アドレス
	通話料無料	• 現在のプロバイダーからの最終請求書 • 認証書 • 勤務先住所 • NRA から入手した証明書 住所は国内でなければならない

英国

以下の表に示すのは、イギリスにおける電話番号の注文と移植の要件の一覧と説明です。

電話番号の注文

サポートされる製品タイプ	番号タイプ	ID の要件	許容 ID タイプ
SIP メディアアプリケーションダイヤルイン	ローカル	いいえ	該当なし
	通話料無料	いいえ	該当なし

電話番号の移植

サポートされる製品タイプ	番号タイプ	必須 ID
SIP メディアアプリケーションダイヤルイン	ローカル	• 現在のプロバイダーからの最終請求書 • 認証書
	通話料無料	• 現在のプロバイダーからの最終請求書 • 認証書

既存の電話番号の移植

> **Important**
>
> 2024 年 3 月 1 日 (金) から、Amazon Chime SDK 電話番号の移植リクエストは、 AWS Support センターコンソールの [アカウントと請求] セクションに移動されました。電話番号の移転に関する新しいサポートケースを作成するには、[アカウントと請求] を選択し、[サービス] ドロップダウンメニューを開いて [Chime (番号管理)] を選択します。

電話番号をプロビジョニングするだけでなく、電話会社の番号を Amazon Chime SDK インベントリに移植することもできます。これには、フリーダイヤル番号も含まれます。Amazon Chime SDK 音声コネクタと Amazon Chime SDK SIP メディアアプリケーションでは、ポート番号を使用できます。

以下のセクションでは、電話番号を移植する方法について説明します。

トピック

番号を移植するための前提条件

番号を移植するには、次のものが必要です。

- エージェンシーレター (LOA)。米国および国際電話番号には LOA が必要です。エージェンシーレター (LOA) フォームをダウンロードして記入してください。電話番号を異なるキャリアから持ち込もうとする場合、キャリアごとに個別の LOA を入力します。

  > **Note**
  >
  > 多くの国では、電話番号の移転に関する書類要件があります。詳細については、このガイドの「国別電話番号要件」を参照してください。

- Amazon Chime SDK 音声コネクタに電話番号を移植する前に、音声コネクタを作成する必要があります。詳細については、「Amazon Chime SDK Voice Connector の作成」を参照してください。

電話番号を Amazon Chime SDK に移植する

既存の電話番号を Amazon Chime SDK に移植するサポートリクエストを作成します。

既存の電話番号を Amazon Chime SDK に移植するには

1. https://console.aws.amazon.com/chime-sdk/home にある Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [お問い合わせ] で、[Support] を選択します。

AWS Support コンソールに移動します。

> **Note**
>
> AWS Support Center ページに直接移動することもできます。その場合は、[ケースを作成] を選択し、以下の手順に従ってください。

3. 「お手伝いできること」で、次の操作を行います。

   a. [Account and billing] (アカウントおよび請求) を選択します。

   b. 「サービス」リストから「Chime SDK (番号管理)」を選択します。

   c. 「カテゴリ」リストから「電話番号」「ポートイン」を選択します。

   d. [Next step: Additional information] (次のステップ:追加情報) を選択します。

4. [追加情報] で、次の操作を行います。

   a. [件名] に **`Porting phone numbers in`** と入力します。

   b. [説明] に、次の情報を入力します。

      米国番号を移植する場合:

      - アカウントの請求電話番号 (BTN)。
      - ユーザーの名前の承認。これは、現在のキャリアでアカウント請求を担当する人物です。
      - 現在のキャリア (既知の場合)。
      - サービスアカウント番号 (この情報が現在のキャリアに存在する場合)。
      - サービス PIN (使用可能な場合)。
      - 現在のキャリア契約に表示されるサービス住所と顧客名。
      - 移植をリクエストした日時。
      - (オプション) BTN を移植する場合、以下のオプションのいずれかを指定します。
        - 現在の BTN を移植し、提供する新しい BTN に置き換える。この新しい BTN が現在のキャリアのアカウントの BTN になる。
        - 現在の BTN を移植し、現在のキャリアのアカウントを閉鎖する。
        - 現在のアカウントで各電話番号がそれぞれ BTN になるように設定されているため、現在の BTN を移植する。(このオプションは、現在のキャリアのアカウントがこの方法で設定されている場合にのみ選択します)

- 上記のオプションのいずれかを選択したら、依頼書に委任状 (LOA) を添付してください。

国際番号を移植する場合:

- 米国以外の番号の場合、SIP メディアアプリケーションダイヤルイン製品タイプを使用する必要があります。
- 番号のタイプ (市内または通話料無料)
- 持ち込もうとする既存の電話番号。
- 使用量の推定
- 国

c. 電話番号タイプリストから、「ビジネスコール」、「SIP メディアアプリケーションダイヤルイン」、または「音声コネクタ」を選択します。

d. [電話番号] には、複数の電話番号を移植する場合でも、少なくとも 1 つの電話番号を入力します。

e. [移植日] に、希望する移植日を入力します。

f. 「移植時間」に、希望する時間を入力します。

g. [次のステップ: 今すぐ解決またはお問い合わせ] を選択します。

5. [今すぐ解決] または [お問い合わせ] で [お問い合わせ] を選択します。
6. 「優先問い合わせ言語」リストから、言語を選択します。
7. [Web] または [電話] を選択します。[電話] を選択した場合は、電話番号を入力します。終了したら、[送信] を選択します。

AWS Support 電話番号を既存の電話キャリアから移管できるかどうかを知らせます。可能であれば、必要な書類をすべて提出する必要があります。次のセクションでは、これらの書類の提出方法を説明します。

必要書類の提出

AWS 電話番号を移植できるとSupport から通知されたら、必要な書類をすべて提出する必要があります。以下では、その手順を説明します。

> **Note**
>
> AWS Support では、リクエストされたすべてのドキュメントをアップロードするための安全な Amazon S3 リンクを提供しています。リンクを受け取るまで先に進まないでください。

書類を提出するには

1. https://console.aws.amazon.com/chime-sdk/home にある Amazon Chime SDK コンソールを開きます。
2. アカウントにサインインし、 AWS アカウント専用に生成された Amazon S3 アップロードリンクを開きます。

   > **Note**
   >
   > このリンクは 10 日後に期限切れになります。このリンクは、ケースを作成したアカウント専用に生成されます。このリンクには、アカウントの権限を持つユーザーがアップロードを実行する必要があります。

3. [ファイルを追加] を選択し、リクエストに関連する身分証明書を選択します。
4. 「アクセス許可」セクションを展開し、「個別の ACL アクセス許可の指定」を選択します。
5. アクセス制御リスト (ACL) セクションの最後で、[被付与者を追加] を選択し、 AWS Support から提供されたキーを [被付与者] ボックスに貼り付けます。
6. 「オブジェクト」で「読み取り」チェックボックスを選択し、「アップロード」を選択します。

委任状 (LOA) を提出したら、LOA AWS Support の情報が正しいことを既存の電話会社に確認します。LOA で提供されている情報が、電話キャリアが登録している情報と一致しない場合は、 AWS Support から連絡があり、LOA で提供されている情報を更新するように求められます。

リクエストステータスの表示

Amazon Chime SDK コンソールを使用して移植リクエストのステータスを表示するには。

ステータスを表示するには

1. https://console.aws.amazon.com/chime-sdk/home にある Amazon Chime SDK コンソールを開きます。

2. ナビゲーションペインで [電話番号管理] を選択します。
3. 「注文」タブを選択します。

Status 列にはリクエストのステータスが表示されます。 AWS Support また、必要に応じて、更新情報や詳細情報のリクエストについてお客様に連絡します。詳細については、このセクションの後半の「電話番号の移植ステータスの定義」を参照してください。

ポート番号の割り当て

既存の電話キャリアは、LOA が正しいことを確認した後、リクエストされたポートを確認して承認します。次に、ポートを行う確定注文コミット (FOC) AWS Support の日付と時刻が提示されます。

番号を割り当てるには

1. • Amazon Chime SDK 音声コネクター番号を音声コネクターに割り当ててください。
   • Amazon Chime SDK SIP メディアアプリケーションのダイヤルイン番号の場合は、SIP ルールを使用して番号を割り当てます。SIP ルールの詳細については、「SIP ルールの作成」を参照してください。

   電話番号は、次の手順に示すように注文確定 (FOC) 日が決定されるまで使用可能になりません。詳細については、電話番号インベントリの管理およびAmazon Chime SDK Voice Connector の作成を参照してください。
2.
3. AWS Support FOC に連絡して、日付と時刻が自分に合っていることを確認します。

   > **Note**
   > 電話番号を割り当てるまで通話の発着信はできません。

4. FOC 日に、移植された電話番号は Amazon Chime SDK で使用できるよう有効化されます。

Amazon Chime SDK から電話番号を移植する方法

> **Note**
>
> Amazon Chime SDK から番号を移植できるかどうかは、受信側の通信事業者がその番号を受け入れる能力によって異なります。

既存の電話番号を Amazon Chime SDK に移植するには

1. https://console.aws.amazon.com/chime-sdk/home にある Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [お問い合わせ] で、[Support] を選択します。

   AWS Support コンソールに移動します。

   > **Note**
   >
   > AWS Support Center ページに直接移動することもできます。その場合は、[ケースを作成] を選択し、以下の手順に従ってください。

3. 「お手伝いできること」で、次の操作を行います。
   a. [Account and billing] (アカウントおよび請求) を選択します。
   b. 「サービス」リストから「Chime SDK (番号管理)」を選択します。
   c. 「カテゴリ」リストから「電話番号」「ポートアウト」を選択します。
   d. [Next step: Additional information] (次のステップ:追加情報) を選択します。
4. [追加情報] で、次の操作を行います。
   a. [件名] に **`Porting phone numbers out`** と入力します。
   b. [説明] に、関連するデータを入力します。

AWS Support 新しい通信事業者にポートをリクエストするときに使用するアカウント ID と PIN で応答します。選択した連絡方法と、追加の連絡先について入力した電子メールアドレスに基づいて応答が届きます。

移植プロセスが終了し、電話番号が新しいキャリアに移植されたら、Amazon Chime SDK インベントリから電話番号の割り当てを解除して削除します。詳細については、電話番号インベントリの管理および電話番号を削除するを参照してください。

電話番号の移植ステータスの定義

既存の電話番号を Amazon Chime SDK に移植するリクエストを送信すると、Amazon Chime SDK コンソールの [通話中]、[電話番号管理]、[保留中] で移植リクエストのステータスを確認できます。

移植ステータスと定義は以下のとおりです。

CANCELLED

AWS Support 運送業者またはお客様からのキャンセルリクエストなど、ポートに問題があったため、移植注文をキャンセルしました。 AWS Support 詳細を連絡します。

CANCEL_REQUESTED

AWS Support 運送業者またはお客様からのキャンセル依頼など、港に問題があるため、移植注文のキャンセルを処理している。 AWS Support 詳細を連絡します。

CHANGE_REQUESTED

AWS Support 変更リクエストを処理中で、配送業者の返答は保留中です。処理時間が余分にかかる場合があります。

COMPLETED

移植注文が完了し、電話番号が有効になります。

EXCEPTION

AWS Support 移管リクエストを完了するために必要な追加情報について、お客様に連絡します。処理時間が余分にかかる場合があります。

FOC

FOC 日付は運送業者に確認されます。 AWS Support 日付を確認するためにあなたに連絡します。

PENDING DOCUMENTS

AWS Support ポートリクエストを完了するために必要な追加書類について、お客様に連絡します。処理時間が余分にかかる場合があります。

SUBMITTED

移植注文が送信され、キャリアからの応答待ちです。

電話番号インベントリの管理

以下のセクションの情報では、Amazon Chime SDK 音声コネクタ、Amazon Chime SDK 音声コネクタグループ、および SIP メディアアプリケーションで使用される電話番号をプロビジョニングおよび管理する方法について説明します。

ユーザーの Amazon Chime Business Calling 電話番号または電話番号アクセス許可を変更しようとする場合、新しい電話番号またはアクセス許可情報をユーザーに提供することをお勧めします。ユーザーが新しい電話番号または権限機能にアクセスできるようにするには、Amazon Chime アカウントからサインアウトして再度サインインする必要があります。

トピック

- 音声コネクタまたは音声コネクタグループへの番号の割り当て
- 音声コネクタ番号の再割り当て
- Voice Connectorの電話番号の割り当て解除
- 電話番号の再割り当て
- SIP メディアアプリケーションへの電話番号の割り当て
- 電話番号の詳細を表示する
- 電話番号の製品タイプを変更する
- 電話番号の割り当てタイプを変更します。
- アウトバウンドコール名を設定する

音声コネクタまたは音声コネクタグループへの番号の割り当て

以下の手順では、Amazon Chime SDK 音声コネクタグループと音声コネクタグループに電話番号を割り当てる方法を説明します。番号を割り当てると、電話をかけることができます。

音声コネクタと音声コネクタグループには、個別の番号または番号グループを割り当てることができます。以下では、その手順を説明します。

個別の電話番号を割り当てるには

1. https://console.aws.amazon.com/chime-sdk/home にある Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [電話番号] で、[電話番号管理] を選択します。
3. 「インベントリ」タブで、割り当てる電話番号を選択し、「編集」を選択します。
4. (オプション)「発信者名」ボックスに、電話番号の名前を入力します。
5. 「製品タイプ」で、「Voice Connector」が選択されていることを確認します。
6. [課題タイプ] で [音声コネクタ] または [音声コネクタグループ] を選択し、次のいずれかを実行します。
   a. 「音声コネクタ」を選択した場合は、「音声コネクタ」オプションリストを開いて、音声コネクタを選択します。
   b. Voice Connectorグループを選択した場合は、Voice Connectorグループのオプションリストを開いて、Voice Connectorグループを選択します。
7. [保存] を選択します。

電話番号のグループを割り当てるには

1. 「インベントリ」タブで、割り当てる電話番号の横にあるチェックボックスを選択します。

> **Note**
>
> 電話番号には Voice Connector 製品タイプが必要です。また、「ステータス」列をチェックして、割り当てられていない番号のみを選択するようにしてください。

2. [割り当て] を選択し、[割り当てタイプ] ダイアログボックスで [音声コネクタ] または [音声コネクタグループ] を選択します。
3. 「割り当て」を選択し、「電話番号の割り当て」ダイアログボックスで「音声コネクタ」または「音声コネクタグループ」を選択し、「次へ」を選択します。
4. 「音声コネクタ」または「音声コネクタ」グループを選択し、「割り当て」を選択します。

音声コネクタ番号の再割り当て

ある Amazon Chime SDK 音声コネクタグループまたは Amazon Chime SDK 音声コネクタグループから別のグループに電話番号を再割り当てできます。番号には音声コネクタの製品タイプが必要です。

個別の番号または番号のグループを再割り当てできます。次の手順では、両方の方法について説明しています。

個別の番号を再割り当てするには

1. https://console.aws.amazon.com/chime-sdk/home にある Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [電話番号] で、[電話番号管理] を選択します。
3. 「インベントリ」タブで、再割り当てする電話番号を選択します。
4. [編集] を選択します。
5. 「課題タイプ」で、「音声コネクタ」または「音声コネクタグループ」を選択します。次に。
6. 次のいずれかを行います。
    a. 音声コネクタを選択した場合は、音声コネクタオプションリストを開き、新しい音声コネクタを選択します。
    b. Voice Connectorグループを選択した場合は、Voice Connectorグループのオプションリストを開き、新しいVoice Connectorグループを選択します。
7. [保存] を選択します。

電話番号のグループを再割り当てするには

1. https://console.aws.amazon.com/chime-sdk/home にある Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [電話番号] で、[電話番号管理] を選択します。
3. 「インベントリ」タブで、再割り当てする電話番号の横にあるチェックボックスを選択し、「再割り当て」を選択します。
4. 「再割り当て」ダイアログボックスで、「音声コネクタ」または「音声コネクタ」グループを選択し、「次へ」を選択します。
5. 音声コネクタまたは音声コネクタグループを選択し、「再割り当て」を選択します。

Voice Connectorの電話番号の割り当て解除

以下の手順では、Amazon Chime SDK 音声コネクタグループと音声コネクタグループから電話番号の割り当てを解除する方法について説明します。SIP メディアアプリケーションで使用されている電話番号は割り当て解除できません。代わりに SIP ルールを削除します。SIP ルールの削除について詳しくは、SIP ルールの削除本ガイドのを参照してください。

> **Note**
>
> 番号の割り当てを解除して SIP ルールを削除すると、ユーザーのテレフォニー機能は無効になります。ただし、割り当てられていない番号はインベントリに残り、その製品タイプに応じて請求されます。

Voice Connectorの電話番号の割り当てを個別に解除するには

1. https://console.aws.amazon.com/chime-sdk/home にある Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [電話番号] で、[電話番号管理] を選択します。
3. 「インベントリ」タブで、割り当てを解除する電話番号を選択します。
4. [編集] を選択し、[割り当てタイプ] で [音声コネクタ] または [音声コネクタグループ] を選択します。
5. 音声コネクタオプションまたは音声コネクタグループのオプションリストを開き、リストの最初のオプションである [なし (割り当て解除)] を選択します。

電話番号の再割り当て

Amazon Chime SDK 音声コネクタまたは音声コネクタグループに電話番号を割り当てたら、番号の割り当てを解除しなくても、その番号を別の音声コネクタまたはグループに再割り当てできます。

電話番号を再割り当てするには:

1. https://console.aws.amazon.com/chime-sdk/home にある Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [電話番号] で、[電話番号管理] を選択します。
3. 再割り当てする番号の横にあるチェックボックスを選択し、[再割り当て] を選択します。 。

4. 再割り当てダイアログボックスで、「音声コネクタ」または「音声コネクタ」グループを選択し、「次へ」を選択します。
5. 目的の音声コネクタまたは音声コネクタグループを選択し、「再割り当て」を選択します。

SIP メディアアプリケーションへの電話番号の割り当て

SIP メディアアプリケーションに電話番号を割り当てるには、アプリケーションに関連付けられている SIP ルールに電話番号を追加します。詳細については、「SIP メディアアプリケーションの管理」を参照してください。

電話番号の詳細を表示する

インベントリの電話番号の詳細を表示するのにはいくつかの理由があります。たとえば、番号が割り当てられている音声コネクタや SIP メディアアプリケーションを表示できます。テキストメッセージが有効になっているかどうかも確認できます。

電話番号の詳細を表示するには

1. https://console.aws.amazon.com/chime-sdk/home にある Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [電話番号] で、[電話番号管理] を選択します。
3. 「インベントリ」タブで、表示したい電話番号を選択します。

> **Note**
>
> 以下の操作を行うこともできます。
>
> 1. 表示したい電話番号の横にあるチェックボックスを選択します。
> 2. [アクション] リストを開いて [詳細を表示] を選択します。

電話番号の製品タイプを変更する

Amazon Chime SDK 音声コネクタの電話番号を割り当てていない場合は、その電話番号をある製品タイプから別の製品タイプに切り替えることができます。

> **Note**
>
> 米国以外の電話番号の場合は、SIP メディアアプリケーションダイヤルイン製品タイプを使用する必要があります。

製品タイプを変更するには

1. https://console.aws.amazon.com/chime-sdk/home にある Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [電話番号] で、[電話番号管理] を選択します。
3. 「インベントリ」タブで、変更する電話番号を選択します。
4. [Details (詳細)] ページで、[Edit (編集)] を選択します。
5. 「製品タイプの編集」ダイアログボックスで、「Voice Connector」または「SIP メディアアプリケーションダイヤルイン」を選択し、「保存」を選択します。

電話番号の割り当てタイプを変更します。

Amazon Chime SDK 音声コネクタまたは Amazon Chime SDK SIP メディアアプリケーションの電話番号の割り当てを解除している場合は、それらをある製品タイプから別の製品タイプに切り替えることができます。

> **Note**
>
> 米国以外の電話番号の場合は、SIP メディアアプリケーションダイヤルイン製品タイプを使用する必要があります。

アサインメントタイプを変更するには

1. https://console.aws.amazon.com/chime-sdk/home にある Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [電話番号] で、[電話番号管理] を選択します。
3. 「インベントリ」タブで、変更する電話番号を選択します。
4. [Details (詳細)] ページで、[Edit (編集)] を選択します。

5. 「課題タイプ」で、「音声コネクタ」または「音声コネクタグループ」を選択します。

   選択内容に応じて、「音声コネクター」オプションまたは「音声コネクターグループ」オプションリストが表示されます。

6. リストを開いて、音声コネクタまたは音声コネクタグループを選択します。
7. [保存] を選択します。

アウトバウンドコール名を設定する

インベントリ内の電話番号に発信者名を割り当てることができます。これはフリーダイヤル番号にのみ適用され、フリーダイヤル番号は対象外です。名前はアウトバウンドコールの受信者に表示されます。名前は 7 日ごとに更新できます。

> **Note**
>
> Amazon Chime SDK 音声コネクタを使用して電話をかけると、その通話は公衆交換電話網を経由して着信側の電話キャリアにルーティングされます。発信者 ID 名をサポートしていない通信事業者もあれば、音声コネクタの CNAM データベースを使用しない通信事業者もあります。そのため、着信側には発信者名が表示されない場合や、設定した発信者名とは異なる発信者名が表示される場合があります。
> 米国の通信事業者は、大量の通話、ショートコール、未応答コールなど、スパムや詐欺の特徴を示す電話番号をブロックしたり、ラベルを付けたりするケースが増えています。通話が同様に分類されるリスクを減らすには、発信通話を無料発信者登録サービスに登録することを検討してください。

以下では、発信者名を追加する手順を説明します。

アウトバウンドコール名を設定するには

1. https://console.aws.amazon.com/chime-sdk/home にある Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [電話番号] で、[電話番号管理] を選択します。
3. 「インベントリ」タブで、名前を追加したい番号を選択します。
4. [Details (詳細)] ページで、[Edit (編集)] を選択します。
5. [発信者名] ボックスに、名前を入力します。15 文字まで使用できます。

6. [保存] を選択します。

システムによって名前が追加されるまで 72 時間かかります。

デフォルトの発信者名を更新するには

- 上記の手順を繰り返します。システムによって名前が更新されるまで 72 時間かかります。

電話番号を削除する

> **Important**
>
> 電話番号を削除する前に、割り当てを解除する必要があります。次のいずれかを行います。
>
> - Voice Connector または Voice Connector グループを使用している場合は、電話番号の割り当てを解除します。詳細については、本ガイドの「Voice Connectorの電話番号の割り当て解除」を参照してください。
> - SIP メディアアプリケーションを使用している場合は、その電話番号が含まれる SIP ルールを削除します。詳細については、本ガイドの「SIP ルールの削除」を参照してください。

番号を削除すると、その番号は削除キューに移動し、7 日間保持されます。その間は、電話番号をインベントリに戻すことができます。7 日間経過すると、その電話番号は自動的に保持キューから削除され、アカウントとの関連付けが解除されます。これにより、その電話番号は Amazon Chime SDK の番号プールに返されます。保持キューから電話番号が削除された後でその番号を再申請する必要がある場合は、電話番号のプロビジョニング の手順に従ってください。ただしその番号は使用できない可能性があることに注意してください。

未割り当ての電話番号を削除するには

1. https://console.aws.amazon.com/chime-sdk/home にある Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [電話番号] で、[電話番号管理] を選択します。
3. 「インベントリ」タブで、削除する番号を選択し、「削除」を選択します。
4. 「電話番号を削除」ダイアログボックスで、「このアクションの影響を理解しています」の横にあるチェックボックスを選択し、「削除」を選択します。

システムは、削除された電話番号を削除キューに 7 日間保持し、その後完全に削除します。

削除された電話番号の復元

電話番号の削除後、最大で 7 日までは [Deletion queue (削除キュー)] から削除された電話番号を復元できます。電話番号を復元すると、これは [インベントリ] に戻されます。

7 日間の期間が過ぎると、削除キューによって番号が番号プールに戻ります。

削除された電話番号を復元するには

1. https://console.aws.amazon.com/chime-sdk/home にある Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [電話番号] で、[電話番号管理] を選択します。
3. [削除キュー] タブを選択し、復元する 1 つまたは複数の電話番号を選択します。
4. [Move to inventory (インベントリに移動)] を選択します。

発信通話の評価を最適化する

発信ビジネスコールを行う場合、最も難しいタスクの 1 つは、顧客がダイヤルアウトしたときにコールに応答しない理由を理解することです。顧客はわざと応答しなかったのか、それとも仕事の電話や来客の対応で忙しいのか? 企業にとっては知ることは不可能ですが、通話の成功率を高めるための対策を講じることができます。

以下のトピックでは、発信通話の応答率を向上させる方法を推奨しています。

トピック

ステップ 1: 顧客が好む連絡方法を知る

企業が行う最大の間違いの 1 つは、顧客が電話による連絡を希望するかどうかわからないことです。顧客があなたと関わったとき、電話、電子メール、またはテキストで連絡を取りたいかどうかを確認しましたか?

マルチチャネルエンゲージメントのある企業は、マルチチャネルエンゲージメントを持たない企業と比較して、平均で 70% 上回っています。

ステップ 2: 通話をブランド化する

コールブランディングソリューションを使用することにより、会社名、ロゴ、電話の理由、サービスを含め、より充実した通話ディスプレイを提供できます。通話をブランド化すると、通話応答率が 30% 向上する可能性があります。

Amazon Chime SDK と Amazon Connectは、ファーストオリジンや Neustar などのソリューションプロバイダーと提携して、ブランド通話サービスを提供しています。パートナーと直接サービスについて説明するには、パートナーのウェブサイトにアクセスしてください。

- 最初のオリジン
- Neustar

ステップ 3: 顧客にとって意味のある発信者 ID を選択する

すべてのビジネスが同じというわけではありません。一部の人にとってはうまくいくものが、他の人にとってはうまくいかないかもしれません。ただし、発信者 ID に基づくアウトバウンドキャンペーンの成功率には相関関係があります。以下の提案は、わかりやすい発信者 IDsを作成するのに役立ちます。

- エリアローカリゼーション。見込み客と同じエリアの発信者 ID を使用します。
- 都市のローカリゼーション。見込み客と同じエリアの発信者 ID を使用します。
- 0800 123 0000 などの認識可能なゴールデン通話料無料番号。

ステップ 4: キャンペーンで有効な電話番号に電話をかけることを確認する

多くの企業には、顧客の詳細を更新するプロセスがありません。これまで以上に多くのモバイルユーザーにとって、企業が連絡先情報を更新することは不可欠です。顧客が電話に応答しない場合は、Amazon Pinpoint を使用して電話番号 を検証することをお勧めします。顧客が、電話している電話番号にいなくなった可能性があります。

ステップ 5: 最適なタイミングで発信通話を行う

最適なタイミングで通話が発信されていることを確認します。一般的に、午前 10 時の前または午後 5 時以降に電話をかけないでください。最も多用中であるか、クワイエットタイムが必要なためです。顧客のプロフィールにもよりますが、顧客にとって都合の良いときに電話をかける必要があります。これは、ある顧客が正午に、別の顧客が午後に電話をかけることを意味します。

さらに、TCPA (米国) や OFCOM (英国) などの規制では、エンドカスタマーに電話をかけないタイミングに関するガイダンスも提供しています。このような規制に従うことを強くお勧めします。

ステップ 6: 発信者 ID の評価を監視する

Free Caller Registry などのサービスを通じて、発信者 IDs の評価をモニタリングすることをお勧めします。

最も正当なアウトバウンドコールキャンペーンでも、十分な電話をかけると、一部のユーザーは発信者 ID にスパムのフラグを付けます。これは 2 つの方法で明らかになります。

1. 自動ブロッキング。ブロックリストは vendor-by-vendor ベースで実装されます。例えば、Samsung デバイスの Hiya.com などのアプリケーションプロバイダーでレポートが一定のしきい値に達すると、最大 20% の見込み客がすぐに連絡不能になります。
2. 苦情。ユーザーは、多数のウェブサイトを使用して、特定の発信者 IDsからの通話について苦情を送信できます。多くの見込み客は、電話を受けたときに発信者 ID をオンラインで検索します。評判が悪いと、応答する可能性が低くなります。

フラグが立てられた発信者 ID から回復する最も速い方法は、新しい電話番号に切り替えることです。次のステップを参照してください。

ステップ 7: 複数の番号を発信者 ID として使用する

現在、企業は通常、インテリジェントで効率的なダイヤル方法を採用しています。

例えば、1 つの方法では、発信通話を行うときに複数の電話番号を使用します。同じ番号から繰り返し電話がかかってきていると感じない場合、顧客が電話に応答する可能性が高くなります。

ステップ 8: アプリベンダーと連携する

現在の業界で最も難しい問題の 1 つは、多数のベンダーが通話をブロックするアプリ内サービスを提供していることです。これらのアプリ内サービスのいずれかが番号をスパムとしてマークする場合は、スパムリストから番号を削除するためにプレミアム料金を支払います。

一部のサードパーティベンダーは、通話応答率を高めるために提携しています。

ステップ 9: アウトリーチ戦略にメッセージを追加して、あなたが誰であるかを顧客に知らせる

通話が応答しない場合は、SMS を使用して見込み者に問い合わせることができます。次のアイデアを試して、回答率を増やしてください。

1. を呼び出す前に、お客様が誰であり、いつ電話するかを顧客に指示する SMS を送信します。オプションで、顧客はより便利な時間に再スケジュールできます。
2. 見込み客が応答しない場合は、SMS を送信して、電話のスケジュールを変更するか、折り返し電話を要求できるようにします。
3. プロモーションオファーや割引を利用して、顧客の期待に反応させます。

ステップ 10: 発信通話戦略を検証する

データ主導の意思決定を行い、継続的に反復することで、真のビジネス価値を実現できる可能性が最も高くなります。アウトバウンド通話戦略の各変更を実験として扱い、変更の有効性を測定および比較できるようにします。

Amazon Connect の最も優れている点の 1 つは、サービスをすぐに実験できることです。ベースラインを確立し、変更を比較して、どのように成功できるかを評価できます。

Amazon Chime SDK Voice Connector の管理

Amazon Chime SDK Voice Connector とは

Amazon Chime SDK Voice Connector は、既存の電話システムにセッション開始プロトコル (SIP) トランキングサービスを提供します。Voice Connector は、Amazon Chime SDK コンソールから管理してインターネット接続経由でアクセスすることも、 を使用することもできますAWS Direct Connect。詳細については、『AWS Direct Connect ユーザーガイド』の「What is AWS Direct Connect? (とは？)」 を参照してください。

> **Important**
>
> Voice Connector は SMS をサポートしていません。

Voice Connector の発信通話と着信通話

Voice Connector を作成したら、終了と発信の設定を編集して、発信通話または着信通話、またはその両方を許可します。次に、電話番号を Voice Connector に割り当てます。Amazon Chime SDK コンソールを使用して、既存の電話番号を移行したり、新しい電話番号をプロビジョニングしたりできます。詳細については、「既存の電話番号の移植」、「電話番号のプロビジョニング」、および「Amazon Chime SDK Voice Connector 電話番号の割り当てと割り当て解除」を参照してください。

> **Note**
>
> - Amazon Chime SDK Voice Connector には、アウトバウンドの国際通話制限があります。詳細については、「発信通話の制限」を参照してください。
> - Voice Connector は E.164 形式の発信通話をサポートしており、011 などの国際ダイヤルアクセスコードは必要ありません。通話料は通話相手の国に基づいて分単位で発生します。現在サポートされている国の一覧および各国の分単位の通話料については、https://aws.amazon.com/chime/voice-connector/pricing/ を参照してください。Voice Connector PSTN 呼び出しは、4、5、または 6 桁の拡張番号などのプライベート番号付けスキームをサポートしていません。

Voice Connector グループ

Voice Connector グループを作成して Voice Connector を追加することもできます。異なるリージョンで作成された Voice Connector AWS を使用できます。これにより、可用性イベントが発生した場合にフォールバックに切り替える耐障害性メカニズムが構築されます。詳細については、「Amazon Chime SDK Voice Connector グループの管理」を参照してください。

Voice Connector データのログ記録とモニタリング

オプションで、Voice Connector から CloudWatch Logs にログを送信し、Amazon Chime SDK Voice Connector から Amazon Kinesis へのメディアストリーミングを有効にできます。詳細については、「CloudWatch Amazon Chime SDK の ログ」および「Amazon Chime SDK Voice Connector メディアを Kinesis にストリーミングする」を参照してください。

目次

開始する前に

Amazon Chime SDK Voice Connector を使用するには、IP プライベートブランチ交換 (PBX)、セッションボーダーコントローラー (SBC)、またはセッション開始プロトコル (SIP) をサポートするインターネットアクセスを持つその他の音声インフラストラクチャが必要です。ピーク時の通話量をサポートするだけの十分な帯域幅があることを確認します。帯域幅の要件については、「帯域幅の要件」を参照してください。

AWS からオンプレミス電話システムへの通話の送信におけるセキュリティを確保するため、AWS と使用する電話システム間に SBC を設定することが推奨されます。Amazon Chime SDK Voice Connector シグナリングおよびメディア IP アドレスから SBC への SIP トラフィックを一覧表示で

きるようにします。詳細については、「Amazon Chime SDK Voice Connector」で推奨されるポートおよびプロトコルを参照してください。

Amazon Chime SDK Voice Connector では、電話番号が E.164 形式であることを想定しています。

Amazon Chime SDK Voice Connector の作成

Amazon Chime SDK コンソールを使用して Amazon Chime SDK Voice Connector を作成します。

Voice Connector を作成するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの SIP Trunking で、音声コネクタ を選択します。
3. [Create new voice connector (新しい音声コネクタの作成)] を選択します。
4. 音声コネクタ名 に、音声コネクタの名前を入力します。
5. 暗号化 で、有効または無効 を選択します。
6. (オプション) タグ で、新しいタグ を追加 を選択し、次の操作を行います。
   1. キー に、タグのキーを入力します。
   2. 値 に、タグの値を入力します。
   3. 必要に応じて、新しいタグを追加 を選択して、Voice Connector にさらにタグを追加します。

   タグの詳細については、「」を参照してくださいVoice Connector へのタグの追加。
7. Voice Connector の作成を選択します。

> **Note**
>
> 暗号化を有効にすると、Voice Connector が SIP シグナリングに TLS トランスポートを使用し、メディアにセキュア RTP (SRTP) を使用するように設定されます。受信通話は TLS トランスポートを使用し、暗号化されていない発信通話はブロックされます。

Voice Connector でのタグの使用

このセクションのトピックでは、既存の Amazon Chime SDK Voice Connector でタグを使用する方法について説明します。タグを使用すると、Voice Connector などのAWSリソースにメタデータを割り当てることができます。タグは、リソースに関する情報、またはそのリソースに保持されているデータを保存するキーとオプションの値で構成されます。すべてのキーと値を定義します。例えば、 という名前のタグキーを の値`CostCenter`で作成`98765`し、そのペアをコスト配分に使用できます。Voice Connector には最大 50 個のタグを追加できます。

Voice Connector へのタグの追加

既存の Amazon Chime SDK Voice Connector にタグを追加できます。

Voice Connector にタグを追加するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [SIP トランキング] で、[Voice Connector] を選択します。
3. 使用する Voice Connector の名前を選択します。
4. [タグ] タブ、[タグを管理] の順に選択します。
5. 新しいタグを追加を選択し、キーとオプションの値を入力します。
6. 必要に応じて、新しいタグを追加を選択して別のタグを作成します。
7. 完了したら、[変更を保存] を選択します。

タグの編集

必要なアクセス許可がある場合は、誰がタグを作成したかにかかわらず、AWSアカウント内の任意のタグを編集できます。ただし、IAM ポリシーでは、これを行うことができない場合があります。

タグを編集するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [SIP トランキング] で、[Voice Connector] を選択します。
3. 使用する Voice Connector の名前を選択します。

4. [タグ] タブ、[タグを管理] の順に選択します。
5. キーまたは値 ボックスに新しい値を入力します。
6. 完了したら、[変更を保存] を選択します。

タグの削除

必要なアクセス許可がある場合は、誰がタグを作成したかにかかわらず、AWSアカウント内のタグを削除できます。ただし、IAM ポリシーでは、これを行うことができない場合があります。

タグを削除するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [SIP トランキング] で、[Voice Connector] を選択します。
3. 使用する Voice Connector の名前を選択します。
4. [タグ] タブ、[タグを管理] の順に選択します。
5. 削除するタグの横にある 削除を選択します。
6. [変更の保存] をクリックします。

Amazon Chime SDK Voice Connector 設定の編集

Amazon Chime SDK Voice Connector を作成したら、発信通話と発信通話を許可する終了設定と発信元設定を編集する必要があります。Kinesis へのストリーミングや緊急通報ルーティングの使用など、他の多くの設定を行うこともできます。Amazon Chime コンソールを使用して、すべての設定を編集します。

Amazon Chime SDK Voice Connector の設定を編集するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの SIP Trunking で、音声コネクタ を選択します。
3. 編集する Amazon Chime SDK Voice Connector の名前を選択します。
4. Amazon Chime コンソールは、一連のタブで Voice Connector 設定をグループ化します。各タブの使用については、以下のセクションを展開してください。

全般設定の編集

全般タブを使用して、Voice Connector の名前を変更し、暗号化を有効または無効にし、ワイルドカードルート証明書を SIP インフラストラクチャにインポートします。

一般的な設定を変更するには

1. (オプション) 詳細 で、Voice Connector の新しい名前を入力します。
2. (オプション) 暗号化 で、有効または無効 を選択します。暗号化の詳細については、次のセクションを展開してください。
3. [Save] (保存) を選択します。
4. (オプション) ワイルドカードルート証明書をダウンロードするには、こちらをダウンロードリンクを選択します。SIP インフラストラクチャに追加する方法がわかっていることを前提としています。

Voice Connector での暗号化の使用

Amazon Chime SDK Voice Connector の暗号化を有効にすると、SIP シグナリングに TLS を使用し、メディアには Secure RTP (SRTP) を使用します。Voice Connector サービスは TLS ポート 5061 を使用します。

有効にすると、すべてのインバウンドコールは TLS を使用し、暗号化されていないアウトバウンドコールはブロックされます。Amazon Chime ルート証明書をインポートする必要があります。Amazon Chime SDK Voice Connector サービスは、米国リージョンおよびその他の`*.region.vc.chime.aws`リージョン`*.voiceconnector.chime.aws`でワイルドカード証明書を使用します。例えば、このサービスはアジアパシフィック (シンガポール) リージョン`*.ap-southeast-1.vc.chime.aws`で を使用します。RFC 4568 で説明されているように SRTP を実装しています。

> **Note**
>
> Voice Connector が TLS 1.2 をサポート

アウトバウンドコールの場合、サービスは SRTP のデフォルトAWSカウンター暗号と HMAC-SHA1 メッセージ認証を使用します。インバウンド通話とアウトバウンド通話では、次の暗号スイートがサポートされています。

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- AES_CM_192_HMAC_SHA1_80
- AES_CM_192_HMAC_SHA1_32
- AES_CM_256_HMAC_SHA1_80
- AES_CM_256_HMAC_SHA1_32

少なくとも 1 つの暗号を使用する必要がありますが、Voice Connector 暗号化には追加料金なしで、優先順に含めることができます。

また、以下の追加の TLS 暗号スイートもサポートしています。

- AES256-GCM-SHA384
- AES256-SHA256
- AES256-SHA
- AES128-GCM-SHA256
- AES128-SHA256
- AES128-SHA
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256

終了設定の編集

終了設定を使用して、Amazon Chime SDK Voice Connector からの発信通話を有効にして設定します。

> **Note**
>
> アウトバウンドホスト名は、EC2 インスタンスがサービスに出入りするときに変更される可能性がある一連の IP アドレスに解決されるため、DNS の有効期限よりも長くレコードをキャッシュしないでください。長期間にわたってキャッシュすると、通話が失敗することがあります。

[Save (保存)] を再度選択します。

終了設定を編集するには

1. [Enabled] (有効) を選択します。
2. (オプション) 許可ホストリスト で、新規 を選択し、許可する CIDR 表記と値を入力して、 を追加 を選択します。IP アドレスの値はパブリックにルーティング可能なアドレスである必要があることに注意してください。

   -もしくは-

   CIDR 表記の編集と変更を選択します。

   -もしくは-

   削除を選択してホストを削除します。
3. 「1 秒あたりの呼び出し数」で、使用可能な場合は別の値を選択します。
4. 通話プラン で国リストを開き、Voice Connector が通話できる国を選択します。
5. 「認証情報」で「新規」を選択し、ユーザー名とパスワードを入力して、「保存」を選択します。
6. 「発信者 ID オーバーライド」で「編集」を選択し、電話番号を選択し、「保存」を選択します。
7. 「最終オプション ping」で、SIP インフラストラクチャによって送信された最後の SIP オプションメッセージを表示します。

発信元設定の編集

発信元設定は、Amazon Chime SDK Voice Connector への着信通話に適用されます。SIP ホストのインバウンドルートを設定して、インバウンドコールを受信できます。受信通話は、ホストごとに設定

した優先度と重量によって SIP インフラストラクチャのホストにルーティングされます。呼び出しは、1 が最優先の優先度順でルーティングされます。ホストが優先度で同等な場合には、呼び出しは相対的な重量に基づいてホスト間に分配されます。

> **Note**
>
> 暗号化が有効な Voice Connectors は、すべての呼び出しに TLS (TCP) プロトコルを使用します。

送信元設定を編集するには

1. [Enabled] (有効) を選択します。
2. インバウンドルート で、新規 を選択します。
3. [ホスト]、[ポート]、[プロトコル]、[優先度]、[Weight (重量)] に値を入力します。
4. [追加] を選択します。
5. [Save] (保存) を選択します。

緊急通報設定の編集

緊急通報を有効にするには、まず終了と発信を有効にする必要があります。これを行う方法については、上記のセクションを参照してください。

これらの手順を完了するには、サードパーティー緊急サービスプロバイダーから少なくとも 1 つの緊急通報ルーティング番号が必要です。数値の取得の詳細については、「」を参照してくださいサードパーティー緊急ルーティング番号の設定。

[追加] を選択します。

緊急通報設定を編集するには

1. [追加] を選択します。
2. 通話送信方法 で、使用可能な場合はリストから項目を選択します。
3. 緊急ルーティング番号を入力します。
4. テストルーティング番号を入力します。テストルーティング番号を取得することをお勧めします。
5. 国 で、可能な場合はルーティング番号の国を選択します。

6. [追加] を選択します。

電話番号の編集

Voice Connector 電話番号の割り当てと割り当て解除を行うことができます。次の手順では、Amazon Chime インベントリに少なくとも 1 つの電話番号があることを前提としています。そうでない場合は、「電話番号のプロビジョニング」を参照してください。

電話番号を割り当てるには

1. [Assign from inventory (インベントリから割り当て)] を選択します。
2. 1 つ以上の電話番号を選択します。
3. [Assign from inventory (インベントリから割り当て)] を選択します。

選択した 1 つ以上の数字が数字のリストに表示されます。

電話番号の割り当てを解除するには

1. 1 つ以上の電話番号を選択します。
2. [割り当て解除] を選択します。
3. オペレーションの確認を求められたら、 の割り当て解除を選択します。

ストリーミング設定の編集

ストリーミング設定は、Amazon Kinesis Video Streams を有効にします。サービスは、ストリーミングオーディオデータを保存、暗号化、およびインデックス化します。

ストリーミング設定を編集するには

1. 詳細 で、開始 を選択します。
2. ストリーミング通知 で、リストから 1 つ以上のターゲットを選択します。
3. データ保持期間 で、データ保持期間なし を選択するか、保持期間を設定します。
4. 「インサイトを呼び出す」で「 をアクティブ化する」を選択し、次の操作を行います。
    1. アクセス許可 で、リストからロールを選択します。
    2. Kinesis Data Stream で、リストからストリームを選択します。

3. (オプション) Amazon Transcribe カスタム言語モデル で、リストからモデルを選択します。
4. 個人を特定できる情報タイプ で、オプションを選択します。
5. 「部分結果のフィルタリング」で、オプションを選択します。
6. 「リアルタイム通知の送信」で「開始」を選択し、「通話方向」と「発話者」リストからオプションを選択します。
7. 必要に応じて、単語/フレーズ を追加を選択し、通知を受け取る単語またはフレーズを入力します。

5. [Save] (保存) を選択します。

ログ記録設定の編集

Amazon Chime SDK は、Voice Connector のログ記録をデフォルトで無効にします。ログ記録を有効にすると、システムは Amazon CloudWatch ロググループにデータを送信します。ログ記録の詳細については、「」を参照してください。 Amazon を使用した Amazon Chime SDK のモニタリング CloudWatch

ログ記録設定を編集するには

1. SIP メトリクスログ で、有効化 を選択します。
2. メディアメトリクスログ で、有効化 を選択します。

タグ設定の編集

Voice Connector には 50 個のタグを追加でき、タグのキーとオプションの値を選択できます。

タグ設定を編集するには

1. [Manage tags (タグの管理)] を選択します。
2. 次のいずれかを実行します。
   - タグを追加するには、新しいタグを追加を選択し、キーとオプションの値を入力します。
   - 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。
3. 完了したら、[変更を保存] を選択します。

Amazon Chime SDK Voice Connector 電話番号の割り当てと割り当て解除

Amazon Chime SDK Voice Connector との間で電話番号の割り当てと割り当て解除を行うことができます。

電話番号を割り当てるには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの SIP Trunking で、音声コネクタ を選択します。
3. Voice Connector の名前を選択します。
4. [電話番号] を選択します。
5. Voice Connector に割り当てる電話番号を 1 つ以上選択します。
6. [Assign (割り当てる)] を選択します。

また、再割り当てを選択して、Voice Connector 製品タイプの電話番号を、ある Voice Connector または Voice Connector グループから別のグループに再割り当てすることもできます。

電話番号の割り当てを解除するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの SIP Trunking で、音声コネクタ を選択します。
3. Voice Connector の名前を選択します。
4. [電話番号] を選択します。
5. Voice Connector から割り当てを解除する電話番号を 1 つ以上選択します。
6. [割り当て解除] を選択します。
7. チェックボックスをオンにし、[割り当て解除] を選択します。

Amazon Chime SDK Voice Connector の削除

Amazon Chime SDK Voice Connector を削除する前に、そのコネクタからすべての電話番号の割り当てを解除する必要があります。Voice Connector からの電話番号の割り当て解除の詳細については、前のトピックを参照してください。

Voice Connector を削除するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの SIP Trunking で、音声コネクタ を選択します。
3. [電話番号]、[Delete voice connector (音声コネクタの削除)] を選択します。
4. チェックボックスをオンにし、[Delete (削除)] を選択します。

通話分析を使用するための Voice Connector の設定

> **Note**
>
> このセクションの手順を完了するには、まず通話分析設定を作成する必要があります。設定の作成については、「」を参照してください通話分析を設定する。

Amazon Chime SDK Voice Connector で Amazon Chime SDK 通話分析を使用すると、Amazon Transcribe でインサイトを自動的に生成し、音声分析で Amazon Transcribe Call Analytics を使用できます。これを行うには、通話分析設定を Amazon Chime SDK 音声コネクタに関連付けます。Voice Connector は、通話ごとに、指定した設定に従って通話分析を呼び出します。1 つの設定を複数の Voice Connector に関連付けることも、Voice Connector ごとに一意の設定を作成することもできます。

Call Analytics は、Amazon Chime Voice Connector のサービスにリンクされたロールを使用して、ユーザーに代わって CreateMediaInsightsPipeline API を呼び出します。

Voice Connector を設定するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [SIP トランキング] で、[Voice Connector] を選択します。

3. 設定に関連付ける Voice Connector の名前を選択し、[ストリーミング] タブを選択します。
4. [開始] を選択していない場合は、それを選択して、Kinesis Video Streams へのストリーミングを開始します。
5. 「コール分析」で「 をアクティブ化」を選択し、表示されるメニューで「コール分析設定 ARN」を選択します。
6. [Save] (保存) を選択します。

> **Note**
>
> Voice Connector に関連付けた設定を有効化、無効化、または変更した後、新しい設定がサービスに反映され有効になるまで 5 分かかります。

Amazon Chime SDK Voice Connector グループの管理

Amazon Chime SDK Voice Connector グループの仕組み

Voice Connector グループは、SIP ベースの電話システムへのインバウンド PSTN 呼び出しのみを処理します。グループは、耐障害性のあるクロスリージョン通話ルーティングを提供します。Voice Connector グループには 2 つ以上の Voice Connector が含まれ、異なるAWSリージョンで作成された Voice Connector を含めることができます。これにより、可用性イベントが 1 つのAWSリージョンのサービスに影響する場合、受信 PSTN 呼び出しをリージョン間でフェイルオーバーできます。

例えば、Voice Connector グループを作成し、米国東部 (バージニア北部) リージョンに 1 つ、米国西部 (オレゴン) リージョンにもう 1 つ、合計 2 つの Voice Connector を割り当てるとします。SIP ホスト (1 つ) を指す発信設定で両方の Voice Connector を設定します。

次に、米国東部 (バージニア北部) リージョンで Voice Connector に電話がかかってくるとします。そのリージョンに接続の問題がある場合、通話は自動的に米国西部 (オレゴン) リージョンの Voice Connector に再ルーティングされます。

Amazon Chime SDK Voice Connector グループの使用を開始する

開始するには、まず異なるAWSリージョンに Voice Connector を作成します。次に、Voice Connector グループを作成し、そのグループに Voice Connector を割り当てます。Amazon Chime SDK 電話番号管理インベントリから Voice Connector グループの電話番号をプロビジョニングすることもできます。詳細については、「電話番号のプロビジョニング」を参照してください。異なる

リージョンでの Amazon Chime SDK Voice Connector の作成の詳細については、AWS「」を参照してくださいAmazon Chime SDK Voice Connector の管理。

目次

Amazon Chime SDK Voice Connector グループの作成

アカウントには、最大 3 つの Amazon Chime SDK Voice Connector グループを作成できます。

グループを作成するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの SIP Trunking で、音声コネクタ を選択します。
3. [グループを作成] を選択します。
4. 表示されるダイアログボックスの音声コネクタグループ名 の下に、グループの名前を入力します。
5. [作成] を選択します。

Amazon Chime SDK Voice Connector グループの編集

Amazon Chime SDK Voice Connector グループを作成したら、そのグループに対して Amazon Chime SDK Voice Connector を追加または削除できます。グループ内の Voice Connector の優先度を編集することもできます。

Voice Connector をグループに追加するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの SIP Trunking で、音声コネクタ を選択します。
3. 編集する Voice Connector グループの名前を選択します。

4. 音声コネクタ タブを選択し、アクション リストを開き、追加 を選択します。
5. 表示されるダイアログボックスで、使用する Voice Connector の横にあるチェックボックスをオンにします。
6. [追加] を選択します。
7. ステップ 4～6 を繰り返して、Voice Connector をグループに追加します。

グループ内の Voice Connector の優先度を編集するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの SIP Trunking で、音声コネクタ を選択します。
3. 編集する Amazon Chime SDK Voice Connector グループの名前を選択します。
4. アクション で、優先度の編集 を選択します。
5. 表示されるダイアログボックスで、Voice Connector ごとに異なる優先順位のランキングを入力します。1 が最も高い優先順位です。優先度の高い Voice Connector が最初に試行されます。
6. [Save] (保存) を選択します。

グループから Voice Connector を削除するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの SIP Trunking で、音声コネクタ を選択します。
3. 編集する Voice Connector グループの名前を選択します。
4. アクションリストを開き、削除を選択します。
5. 表示されるダイアログボックスで、削除する Voice Connector の横にあるチェックボックスをオンにします。
6. [削除] を選択します。

Voice Connector グループへの電話番号の割り当てと割り当て解除

Amazon Chime SDK コンソールを使用して、Voice Connector グループへの電話番号の割り当てと割り当て解除を行います。

Voice Connector グループに電話番号を割り当てるには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの SIP Trunking で、音声コネクタ を選択します。
3. 編集する Voice Connector グループの名前を選択します。
4. [電話番号] を選択します。
5. [Assign from inventory (インベントリから割り当て)] を選択します。
6. Voice Connector グループに割り当てる電話番号を 1 つ以上選択します。
7. [Assign from inventory (インベントリから割り当て)] を選択します。

[Reassign (再割り当て)] を選択して、[Voice Connector (音声コネクタ)] 製品タイプの電話番号を再割り当てすることもできます。これにより、これらの番号をある Voice Connector または Voice Connector グループから別のグループに再割り当てできます。

Voice Connector グループから電話番号の割り当てを解除するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの SIP Trunking で、音声コネクタ を選択します。
3. 編集する Voice Connector グループの名前を選択します。
4. [電話番号] を選択します。
5. Voice Connector グループに必要な電話番号を選択し、 の割り当て解除を選択します。
6. [割り当て解除] を選択します。

Amazon Chime SDK Voice Connector グループの削除

Amazon Chime SDK Voice Connector グループを削除する前に、そのグループからすべての Amazon Chime SDK Voice Connector と電話番号の割り当てを解除する必要があります。詳細については、前の「」セクションを参照してください。

Voice Connector グループを削除するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。

2. ナビゲーションペインの SIP Trunking で、音声コネクタ を選択します。
3. 削除する Voice Connector グループの名前を選択します。
4. [Delete group (グループの削除)] を選択します。
5. チェックボックスをオンにし、[Delete (削除)] を選択します。

Amazon Chime SDK Voice Connector メディアを Kinesis にストリーミングする

分析、機械学習、その他の処理のために、Amazon Chime SDK Voice Connector から Amazon Kinesis Video Streams に通話音声をストリーミングできます。デベロッパーは、音声データを Kinesis Video Streams に保存して暗号化し、Kinesis Video Streams API オペレーションを使用してデータにアクセスできます。詳細については、Kinesis Data Streams デベロッパーガイドを参照してください。

> **Note**
>
> Voice Connector Streaming では、電話番号形式は制限されません。E.164 形式と E.164 以外の形式の番号から通話をストリーミングできます。例えば、Voice Connector ストリーミングは、4、5、または 6 桁の拡張番号、または 11 桁のプライベートワイヤ番号をサポートできます。詳細については、このガイドで後述するSIP ベースのメディア録画とネットワークベースの録画の互換性「」を参照してください。

Amazon Chime SDK コンソールを使用して、Voice Connector のメディアストリーミングを開始します。メディアストリーミングが開始されると、Voice Connector は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用して、Kinesis Video Streams にメディアをストリーミングするアクセス許可を付与します。次に、各 Voice Connector 電話通話レッグからの通話音声がリアルタイムでストリーミングされ、Kinesis Video Streams が分離されます。

Kinesis Video Streams Parser Library を使用して、Voice Connector から送信されたメディアストリームをダウンロードします。次の永続フラグメントメタデータでストリームをフィルタリングします。

- TransactionId
- VoiceConnectorId

詳細については、Amazon Kinesis Video Streams デベロッパーガイドの「Kinesis Video Streams パーサーライブラリ」および「Kinesis Video Streams でのストリーミングメタデータの使用」を参照してください。

Voice Connector での IAM サービスにリンクされたロールの使用の詳細については、「」を参照してくださいAmazon Chime SDK Voice Connector サービスにリンクされたロールポリシーの使用。Amazon Chime SDK CloudWatch で Amazon を使用する方法の詳細については、「」を参照してくださいAmazon Chime SDK でのログ記録とモニタリング。

Voice Connector のメディアストリーミングを有効にすると、Amazon Chime SDK は と呼ばれる IAM サービスにリンクされたロールを作成します AWSServiceRoleForAmazonChimeVoiceConnector。Amazon Chime SDK コンソールで Voice Connector の通話詳細レコードのログ記録を設定している場合、ストリーミング詳細レコードは設定した Amazon S3 バケットに送信されます。詳細については、「Amazon Chime SDK Voice Connector ストリーミング詳細レコード」を参照してください。

メディアストリーミングの開始

Amazon Chime SDK コンソールを使用して、Voice Connector のメディアストリーミングを開始します。

メディアストリーミングを開始するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの SIP Trunking で、音声コネクタ を選択します。
3. Voice Connector の名前を選択します。
4. ストリーミング タブを選択します。
5. 詳細セクションの「Kinesis Video Streams への送信」で、「 の開始」を選択します。
6. データ保持期間 で、 のデータの保持を選択し、保持期間を入力します。
7. [Save] (保存) を選択します。

Amazon Chime SDK コンソールを使用して、メディアストリーミングをオフにします。Voice Connector でメディアストリーミングを使用する必要がなくなった場合は、関連するサービスにリンクされたロールも削除することをお勧めします。詳細については、「Amazon Chime SDK Voice Connector のサービスにリンクされたロールの削除」を参照してください。

Voice Connector のメディアストリーミングを停止するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの SIP Trunking で、音声コネクタ を選択します。
3. Voice Connector の名前を選択します。
4. ストリーミングタブを選択します。
5. 詳細セクションの「Kinesis Video Streams への送信」で、「停止」を選択します。
6. [Save] (保存) を選択します。

SIP ベースのメディア録画とネットワークベースの録画の互換性

Amazon Chime SDK Voice Connector を使用して、Kinesis Video Streams にメディアをストリーミングできます。SIP ベースのメディア録画 (SIPREC) 互換の音声インフラストラクチャまたは Cisco Unified Border Element (CUBE) に関連付けられたネットワークベースの録音 (NBR) 機能からストリーミングできます。

Private Branch Exchange (PBX)、Session Border Controller (SBC)、または SIPREC プロトコルか NBR 機能をサポートするコンタクトセンターが必要です。PBX または SBC は、シグナリングとメディアをAWSパブリック IP アドレスに送信できる必要があります。詳細については、「開始する前に」を参照してください。

SIPREC または NBR で分岐した RTP オーディオストリームのストリーミングを設定するには

1. Voice Connector を作成します。詳細については、「Amazon Chime SDK Voice Connector の作成」を参照してください。
2. Amazon Chime SDK Voice Connector のメディアストリーミングを開始します。詳細については、「メディアストリーミングの開始」を参照してください。
3. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
4. ナビゲーションペインの SIP Trunking で、音声コネクタ を選択します。
5. Voice Connector を選択し、アウトバウンドホスト名 を書き留めます。例えば、*abcdef1ghij2klmno3pqr4*.voiceconnector.chime.aws。
6. 次のいずれかを行います:

- SIPREC の場合 – SIPREC で RTP ストリームを Voice Connector のアウトバウンドホスト名にフォークするように、PBX、SBC、またはその他の音声インフラストラクチャを設定します。
- NBR の場合 – PBX、SBC、またはその他の音声インフラストラクチャを設定して、NBR で RTP ストリームを Voice Connector のアウトバウンドホスト名にフォークします。`X-Voice-Connector-Record-Only` 内の値 `true` を含む `SIP INVITE` の追加のヘッダーまたは URI パラメータを送信します。

Voice Connector での Amazon Chime SDK 音声分析の使用

Voice Connector で Amazon Chime SDK 通話分析を使用して、通話に関するインサイトを自動的に生成します。具体的には、ユーザーを特定し、肯定的、否定的、中立的のいずれかでトーンを予測できます。

通話分析は、Amazon Transcribe、Amazon Transcribe Call Analytics、および Amazon Chime SDK 音声分析で機能します。

このプロセスは、以下の広範なステップに従います。

1. 通話分析設定 を作成します。これは、データの処理手順を含む静的な構造です。
2. 設定を 1 つ以上の Voice Connector に関連付けます。1 つの設定を複数の Voice Connector に関連付けることも、Voice Connector ごとに一意の設定を作成することもできます。
3. Voice Connector は、設定に従って通話分析を呼び出します。

通話分析では、Amazon Chime Voice Connector のサービスにリンクされたロールを使用して、ユーザーに代わって CreateMediaInsightsPipeline API を呼び出します。

> **Note**
>
> 次の手順では、通話分析セッションを Voice Connector に関連付ける方法について説明します。これらを完了するには、まず通話分析設定を作成する必要があります。これを行うには、このガイド通話分析を設定するの「」を参照してください。作成プロセスでは、ARN が設定に割り当てられます。これらのステップで使用する ARN をコピーします。

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。

2. ナビゲーションペインの SIP Trunking で、Voice Connectors を選択し、Voice Connector を選択します。
3. ストリーミングタブを選択します。
4. 「Kinesis Video Streams への送信」で、「 の開始」を選択します。
5. 「コール分析」で、「 をアクティブ化」を選択し、リストから設定を選択し、「保存」を選択します。

Amazon Chime SDK Voice Connector 設定ガイドの使用

Amazon Chime SDK Voice Connector は、幅広いプライベートブランチ交換、セッションボーダーコントローラー、コンタクトセンターシステムでテストされています。これらのテスト済み設定は、一連の設定ガイドで公開されています。

「 設定ガイド」には、各システムテストに使用される設定手順が記載されています。以下のタイプのテストを実行します。

- サードパーティーの SIP プラットフォームから Voice Connector を介した SIP トランキングを有効にします。
- オーディオストリームで使用できるように、Voice Connector 経由で SIPREC を有効にします。

詳細については、「Amazon Chime SDK 設定ガイド」を参照してください。

Amazon Chime SDK 通話分析の管理

セクションのトピックでは、Amazon Chime SDK 通話分析を管理する方法について説明します。通話分析を使用して、リアルタイム音声から通話インサイトを生成します。ストアドコールを分析することもできます。さらに、Amazon Chime SDK 音声分析を使用して発信者を特定し、肯定的、否定的、中立的な感情を予測できます。

トピック

通話分析を設定する

通話分析を使用するには、最初に設定を行います。設定とは、通話分析パイプラインの作成に必要な情報を保持する静的構造を意味します。Amazon Chime SDK コンソールを使用して設定を作成するか、 CreateMediaInsightsPipelineConfiguration API を呼び出すことができます。

通話分析の設定では、録音、音声分析、Amazon Transcribe などの音声プロセッサに関する詳細設定に加え、また、インサイトの送信先とアラートイベント設定も含まれます。必要に応じて、通話データを Amazon S3 バケットに保存し、さらに分析することもできます。

ただし、設定では、特定の音声ソースを指定しません。これにより、その設定を複数の通話分析ワークフローで再利用できます。例えば、同じ通話分析設定を異なる Voice Connector で使用することも、異なる Amazon Kinesis Video Streams (KVS) ソースで使用することもできます。

この設定を使用すると、Voice Connector を介して SIP 通話が発生したとき、または新しいメディアを Amazon Kinesis Video Streams (KVS) に送信するときに、パイプラインを作成できます。これにより、設定内の指定に従って、パイプラインでメディアが処理されます。

パイプラインは、いつでもプログラムで停止できます。Voice Connector の通話が終了すると、パイプラインのメディアの処理は停止します。パイプラインは、一時停止することもできます。これによ

り、基盤となる Amazon 機械学習サービスへの呼び出しを無効にし、必要に応じて再開することが可能です。ただし、パイプラインを一時停止している間も、通話の録音は継続します。

トピック

前提条件

Amazon Transcribe 、Amazon Transcribe Analytics、または Amazon Chime SDK 音声分析で通話分析を使用するには、次の項目が必要です。

- Amazon Chime SDK Voice Connector。そうでない場合は、このガイドの前半のAmazon Chime SDK Voice Connector の作成「」を参照してください。
- Amazon EventBridge ターゲット。そうでない場合は、このガイドの前半のAmazon を使用した Amazon Chime SDK のモニタリング CloudWatch「」を参照してください。
- Voice Connector が EventBridge ターゲット上のアクションにアクセスできるようにするサービスにリンクされたロール。詳細については、このガイドの前半にあるAmazon Chime SDK Voice Connector サービスにリンクされたロールポリシーの使用「」を参照してください。
- 1 つの Amazon Kinesis Data Stream。そうでない場合は、「Amazon Kinesis Video Stream デベロッパーガイド」の「Kinesis Video Stream の作成」を参照してください。 Amazon Kinesis 音声分析と文字起こしには Kinesis ストリームが必要です。
- 通話をオフラインで分析するには、Amazon Chime SDK データレイクを作成する必要があります。これを行うには、「Amazon Chime SDK デベロッパーガイド」の「Amazon Chime SDK データレイクの作成」を参照してください。

通話分析設定の作成

設定を完了したら、Voice Connector をその設定に関連付けて通話分析を有効にします。これにより、その Voice Connector で通話の着信が発生したタイミングで通話分析が自動的に開始されます。詳細については、このガイドの前半にある通話分析を使用するための Voice Connector の設定「」を参照してください。

次のセクションでは、プロセスの各手順を完了する方法について説明します。リストされている項目をこの順序で展開してください。

設定の詳細を指定する

設定の詳細を指定するには、

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [通話分析] で [設定] を選択し、[設定の作成] を選択します。
3. [基本的な情報] で、以下を実行します。

    a. 設定の名前を入力します。ユースケースとタグがわかる名前にする必要があります。

    b. (オプション) [タグ] で [新しいタグの追加] を選択し、タグキーとオプションの値を入力します。キーと値を定義します。タグは、設定のクエリに役立ちます。

    c. [次へ] をクリックします。

録音を設定する

録音を設定するには

- [記録を設定] ページで、次の手順を実行します。

    a. [通話録音を有効にする] チェックボックスを選択します。これにより、Voice Connector の通話や KVS のストリームを録音し、そのデータを Amazon S3 バケットに送信できます。

    b. [ファイル形式] で [WAV と PCM] を選択します。これにより、最良の音質が得られます。

    または

    [OGG と OPUS] を選択すると、音声を圧縮し、ストレージを最適化できます。

    c. (オプション) 必要に応じて、[Amazon S3 バケットの作成] リンクを選択し、次の手順に従って Amazon S3 バケットを作成します。

    d. Amazon S3 バケットの URI を入力するか、[参照] を選択してバケットを検索します。

    e. (オプション) [音声エンハンスメントを有効にする] を選択すると、録音の音質が向上します。

    f. [次へ] をクリックします。

音声機能強化の詳細については、次のセクションを展開してください。

音声エンハンスメントを理解する

音声エンハンスメントは、顧客の Amazon S3 バケットに記録された通話の音声品質を向上させるのに役立ちます。通話は狭いバンドフィルタリングされ、8 kHz のレートでサンプリングされます。音声エンハンスメントでは、サンプリングレートを 8 kHz から 16 kHz に引き上げ、機械学習モデルを使用して周波数成分を狭帯域から広帯域に拡張することで、より自然な音声を実現しています。また、Amazon Voice Focus と呼ばれるノイズリダクションモデルを使用し、拡張機能を使用した音声でバックグラウンドノイズも低減します。

音声エンハンスメントを有効にすると、通話録音の完了後に音声エンハンスメント処理が実行されます。拡張オーディオファイルは元の録音として Amazon S3 バケットに書き込まれ、元の録音の基本ファイル名にサフィックス _enhanced が追加されます。音声エンハンスメントでは、最大 30 分間通話を処理できます。30 分を超える通話では、拡張録音は行えません。

プログラムによる音声エンハンスメントの使用については、「Amazon Chime SDK デベロッパーガイドAPIs を使用して通話分析設定を作成する」を参照してください。

音声機能強化の詳細については、https://docs.aws.amazon.com/chime/latest/dg/ の「Understanding voice enhancements」を参照してください。

分析サービスを設定する

Amazon Transcribe を使用すると、通話の文字起こしを行えます。その後、文字起こししたテキストを使用して、Amazon Comprehend といった他の機械学習サービスや独自の機械学習モデルを強化できます。

> **Note**
>
> Amazon Transcribe は、自動言語認識機能も備えていますが、この機能は、カスタム言語モデルやコンテンツ編集では使用できません。また、他の機能で言語識別を使用する場合は、その機能が対応している言語しか使用できません。詳細については、「Amazon Transcribe Developer Guide」の「Language identification with streaming transcriptions」を参照してください。

Amazon Transcribe Call Analytics は、機械学習を活用した API であり、これによって、通話の文字起こし、センチメント分析、会話に関するインサイトのリアルタイム取得などが可能になります。このサービスを利用すると、メモを取る必要がなくなり、見つかった問題にすぐに対処できます。また、発信者の感情、通話の要因、会話のない時間、会話のさえぎり、会話の速度、会話の特徴などに通話後分析も行えます。

> **Note**
>
> デフォルトの場合、通話後分析は、Amazon S3 バケットにストリーミングされます。録音の重複を防ぐには、通話録音と通話後分析を同時に有効化しないようにします。

さらに、Transcribe Call Analytics では、特定のフレーズに基づいて会話に自動的にタグを付けることで、音声やテキストから機密情報を削除できます。通話分析メディアプロセッサ、これらのプロセッサによって生成されたインサイト、および出力先の詳細については、「Amazon Chime SDK デベロッパーガイド」の「通話分析プロセッサと出力先」を参照してください。

分析サービスを設定するには

1. [分析サービスを設定] ページで、[音声分析] または [文字起こしサービス] の横にあるチェックボックスを選択します。両方の選択も可能です。

   [音声分析] チェックボックスを選択すると、[発話者検索] と [ボイストーン分析] を任意に組み合わせることができます。

   [文字起こしサービス] チェックボックスを選択して、Amazon Transcribe または Transcribe Call Analytics を有効にします。

   a. 発話者検索を有効にするには

      - [はい、Amazon Chime SDK 音声分析の同意確認を認めます] チェックボックスを選択し、[承諾] を選択します。

   b. ボイストーン分析を有効にするには

      - [ボイストーン分析] チェックボックスを選択します。

   c. Amazon Transcribe を有効にするには

      i. [Amazon Transcribe] ボタンを選択します。

      ii. [言語設定] で、次のいずれかを実行します。

         A. 発信者が 1 つの言語を話す場合は、[特定の言語] を選択して [言語] リストを開き、対象の言語を指定します。

         B. 発信者が複数の言語を話す場合は、自動的に識別されます。[言語の自動検出] を選択します。

C. [自動言語識別の言語オプション] リストを開き、少なくとも 2 つの言語を選択します。

D. (オプション) [優先言語] リストを開き、優先言語を指定します。前の手順で選択した言語の信頼スコアが一致すると、優先言語での文字起こしが実行されます。

E. (オプション) [コンテンツ削除設定] を展開して 1 つまたは複数のオプションを選択し、表示される追加オプションから 1 つ以上を選択します。各オプションの説明は、ヘルパーテキストで確認できます。

F. (オプション) [その他の設定] を展開して 1 つまたは複数のオプションを選択し、表示される追加オプションから 1 つ以上を選択します。各オプションの説明は、ヘルパーテキストで確認できます。

d. Amazon Transcribe Call Analytics を有効にするには

i. [Amazon Transcribe Call Analytics] ボタンを選択します。

ii. [言語] リストを開き、言語を選択します。

iii. (オプション) [コンテンツ削除設定] を展開して 1 つまたは複数のオプションを選択し、表示される追加オプションから 1 つ以上を選択します。各オプションの説明は、ヘルパーテキストで確認できます。

iv. (オプション) [その他の設定] を展開して 1 つまたは複数のオプションを選択し、表示される追加オプションから 1 つ以上を選択します。各オプションの説明は、ヘルパーテキストで確認できます。

v. (オプション) [通話後分析] 設定を展開し、次の操作を行います。

A. [通話後分析] チェックボックスを選択します。

B. Amazon S3 バケットの URI を入力します。

C. コンテンツ編集タイプを選択します。

2. 選択したら、[次へ] を選択します。

出力の詳細設定を行う

メディア処理の手順を完了したら、分析結果の出力先を選択します。通話分析では、Amazon Kinesis Data Streams を介して、また、オプションにより、選択した Amazon S3 バケット内のデータウェアハウスを介して、インサイトをライブで取得できます。データウェアハウスを作成するには、 CloudFormation テンプレートを使用します。このテンプレートにより、通話のメタデータとインサイトを Amazon S3 バケットに配信するインフラストラクチャを構築できます。データウェア

ハウスの作成の詳細については、「Amazon Chime SDK デベロッパーガイド」の「Amazon Chime データレイクの作成」および「通話分析データモデル」を参照してください。

設定の作成時に音声分析を有効にすると、AWSLambda、Amazon Simple Queue Service、Amazon Simple Notification Service などの音声分析通知の送信先を追加することもできます。以下では、その手順を説明します。

出力の詳細を設定するには

1. [Kinesis Data Stream] リストを開き、データストリームを選択します。

   > **Note**
   >
   > データを視覚化するには、Amazon S3 バケットと Amazon Kinesis Data Firehose で使用する Kinesis Data Stream を選択する必要があります。

2. (オプション) [その他の音声分析通知先] を展開し、送信先として [AWS Lambda]、[Amazon SNS]、[Amazon SQS] を任意に組み合わせ、選択します。
3. (オプション) [インサイトの分析と視覚化] で、[データレイクを使用した過去データ分析を実行] チェックボックスを選択します。
4. 完了したら、[次へ] を選択します。

アクセス許可を設定する

通話分析を有効にするには、機械学習サービスなどのリソースに、データメディアにアクセスしてインサイトを提供するための権限が必要です。詳細については、「Amazon Chime SDK デベロッパーガイド」の「通話分析リソースアクセスロールの使用」を参照してください。

アクセス許可を設定するには

1. [アクセス許可を設定] ページで、次の操作のいずれかを行います。

   1. [新しいサービスロールを作成し使用する] を選択します。
   2. [サービスロール名のサフィックス] ボックスに、どのようなロールかがわかるようなサフィックスを入力します。

   または

   1. [既存のサービスロールを使用する] を選択します。

2. [サービスロール] リストを開き、ロールを選択します。

2. [次へ] をクリックします。

(オプション) リアルタイムアラートを設定する

> **Important**
>
> リアルタイムアラートを使用するには、まず Amazon Transcribe または Amazon Transcribe Call Analytics を有効にする必要があります。

Amazon にリアルタイムアラートを送信する一連のルールを作成できます EventBridge。Amazon Transcribe または Amazon Transcribe Call Analytics によって生成されたインサイトが、分析セッション中に指定されたルールと一致すると、アラートが送信されます。アラートは 詳細タイプで すMedia Insights Rules Matched。 は、Amazon Lambda、Amazon SQS、Amazon SNS などのダウンストリームサービスとの統合 EventBridge をサポートし、エンドユーザーの通知をトリガーしたり、その他のカスタムビジネスロジックを開始したりします。詳細については、このセクションで後述する「を使用した Amazon Chime SDK の自動化 EventBridge」を参照してください。

アラートを設定するには

1. [リアルタイムアラート] で [リアルタイムアラートを有効にする] を選択します。
2. [ルール] で [ルールを作成] を選択します。
3. [ルール名] ボックスにルールの名前を入力します。
4. [ルールタイプ] リストを開き、使用するルールタイプを選択します。
5. 表示されるコントロールを使用して、ルールにキーワードを追加したり、[言及あり] や [言及なし] などのロジックを適用したりできます。
6. [次へ] をクリックします。

確認と作成

設定を行うには

1. 各セクションの設定内容を確認します。必要に応じて [編集] を選択し、設定を変更します。
2. [Create configuration] (設定を作成) をクリックします。

設定内容は、Amazon Chime SDK コンソールの [設定] ページに表示されます。

通話分析の設定を使用する

設定を作成したら、1 つ以上の Amazon Chime SDK Voice Connector に関連付けて使用します。詳細については、このガイドの前半にある通話分析を使用するための Voice Connector の設定「」を参照してください。

通話分析設定の更新

このセクションのステップでは、通話分析設定を更新する方法について説明します。

設定を更新するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインのコール分析 で、設定 を選択し、更新する設定を選択します。
3. 右上隅の[Edit] (編集) を選択します。
4. 通話分析を設定する 必要に応じて「」の手順に従って、設定を変更します。

   更新された設定と互換性を持たせるようにサービスロールのポリシーを変更するか、新しいサービスロールを選択する必要があります。
5. 完了したら、設定の更新 を選択します。

> **Note**
>
> 設定が Voice Connector に関連付けられている場合、Voice Connector はその設定を自動的に使用します。ただし、音声分析通知ターゲットを有効化、無効化、または調整する場合は、これらの新しい設定が有効になるまで 5 分かかります。

通話分析設定の削除

このセクションのステップでは、Amazon Chime SDK 通話分析設定を完全に削除する方法について説明します。

> **Important**
>
> 削除を元に戻すことはできません。

設定を削除するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインのコール分析 で、設定 を選択し、削除する設定の横にあるラジオボタンを選択します。
3. [削除] をクリックします。
4. 「設定の削除」ダイアログボックスで、**`confirm`**「」と入力して削除を確認し、「削除」を選択します。

音声分析の有効化

> **Important**
>
> この機能を使用する条件として、デジタル音声プロファイル形式の発信者の生体認証識別子と生体認証情報 (「二項データ」) の収集、使用、保存、および保持には、発信者からの文書によるリリースによる同意が必要です。このような同意は、イリノイ州、テキサス州、ワシントン州の生体認証法やその他の州のプライバシー法など、さまざまな州法で義務付けられています。
>
> Amazon Chime SDK 音声分析サービスを使用する前に、各発信者からの同意を明確に反映したプロセスを通じて、各発信者に文書によるリリースを提供する必要があります。これは、サービスの使用AWSの管理に関する同意の条件で求められます。

> **Note**
>
> 音声分析を有効にするには、少なくとも 1 つの Amazon Chime SDK Voice Connector と、少なくとも 1 つの Amazon Chime SDK 通話分析設定が必要です。Voice Connector の作成の詳細については、「」を参照してくださいAmazon Chime SDK Voice Connector の作成。通話

分析設定の作成については、「」を参照してください通話分析を設定する。設定の更新については、「」を参照してください。

このセクションのトピックでは、Amazon Chime SDK Voice Connector の Amazon Chime SDK 音声分析を有効にする方法について説明します。音声分析では、機械学習を使用して、次の一部またはすべてを有効にします。

- 発話者検索 — 発信者の音声をベクトル埋め込みに変換します。次に、埋め込みと既知の音声埋め込みのデータベースを比較します。一致が見つかった場合は、高ライアント音声プロファイル ID 一致のランク付けされたリストと、対応する信頼スコアのセットを返します。

> **Note**
>
> スピーカー検索は、非常に高い精度のスピーカーのアイデンティティを検証するなど、認証や ID 検証のユースケース向けに設計されていません。

- 音声トーン分析 – 言語と音調情報の複合分析に基づいて、音声信号で表現される感情を予測します。

> **Note**
>
> 音声トーン分析を使用する場合は、すべての法的要件を遵守する必要があります。これには、法律の必要に応じてスピーカーから同意を取得する場合や、雇用、住宅、信用価値、財務オファーなど、法的または類似の重大な影響を与えるスピーカーに関する意思決定を行うためにこの機能を使用しない場合が含まれます。

音声分析を有効にするには、管理者は Amazon Chime SDK コンソールを使用して次の操作を行います。

- 上記の 1 つ以上の機能を使用するように Voice Connector を設定します。
- 通知ターゲットを作成します。通知ターゲットは音声分析イベントを非同期的に受信し、少なくとも 1 つのターゲットが必要です。
- 音声プロファイルドメインを作成します。音声プロファイルドメインには、一連の音声プロファイル が含まれています。次に、音声プロファイルは、発信者の音声のベクトル埋め込みと一意の ID で構成されます。デフォルトでは、3 つの音声プロファイルドメインを作成し、各ドメインに

20,000 個の音声プロファイルを格納できます。必要に応じて、両方の制限の引き上げをリクエストできます。

デベロッパーは一連の APIs を使用して、同じタスクを実行できます。詳細については、「Amazon Chime SDK デベロッパーガイド」の「Amazon Chime SDK PSTN 音声分析サービスの使用」を参照してください。

音声プロファイルドメインの管理

Amazon Chime SDK スピーカー検索では、音声プロファイル 、発信者の音声のベクトルマップが作成されます。音声プロファイルドメインは、音声プロファイルのコレクションを表します。デベロッパーが StartSpeakerSearchTask API を呼び出す前に、音声プロファイルドメインを作成する必要があります。

> **Important**
>
> 発話者検索機能には、音声埋め込みの作成が含まれます。これは、発信者の音声を以前に保存した音声データと比較するために使用できます。生体認証識別子と生体認証情報をデジタル埋め込み形式で収集、使用、保存、および保持するには、発信者からの文書によるリリースによる同意が必要になる場合があります。このような同意は、イリノイ州、テキサス州、ワシントン州の生体認証法やその他の州のプライバシー法など、さまざまな州法で義務付けられています。スピーカー検索機能を使用する前に、適用法および機能の使用を規定するAWS サービス条件に従って、すべての通知を行い、すべての同意を得る必要があります。Amazon Chime SDK 音声分析サービスを使用する前に、サービスの使用AWSに関する同意の条件に従って、各発信者の同意を明確に反映したプロセスを通じて、各発信者に文書によるリリースを提供する必要があります。

以下のトピックでは、音声プロファイルドメインを作成および管理する方法を説明します。

トピック

- 音声プロファイルドメインの作成
- 音声プロファイルドメインの編集
- 音声プロファイルドメインの削除
- 音声プロファイルドメインでのタグの使用
- 音声分析の同意通知について

音声プロファイルドメインの作成

このセクションのステップでは、音声プロファイルドメインを作成する方法について説明します。次の点に注意してください。

- ドメイン名は 256 文字を超えることはできません。
- ドメインの説明は 512 文字を超えることはできません。

いずれかの制限を超えると、Amazon Chime SDK コンソールにエラーメッセージが表示されます。

> **Note**
>
> すべてのドメインを暗号化するには、対称 KMS キーを使用する必要があります。詳細については、「音声分析での暗号化の使用」を参照してください。また、エンドユーザーは、音声分析セッションを開始する前に、音声を録音することに同意する必要があります。同意の詳細については、「」を参照してください音声分析の同意通知について。

音声プロファイルドメインを作成するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインで、音声プロファイルドメイン を選択します。
3. 音声プロファイルドメインの作成を選択します。
4. 「承諾」で「はい、Amazon Chime 発話者検索の承諾」を選択します。
5. セットアップ で、ドメインの名前と説明を入力し、KMS キーを選択します。
6. （オプション）タグ で、新しいタグを追加 を選択し、キーとオプションの値を入力します。必要に応じて繰り返し、さらにタグを追加します。
7. 完了したら、音声プロファイルドメインの作成を選択します。

音声プロファイルドメインの編集

誰が作成したかにかかわらず、任意の音声プロファイルドメインを編集できます。

音声プロファイルドメインを編集するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインで、音声プロファイルドメイン を選択します。
3. 編集するドメインの横にあるチェックボックスを選択し、編集を選択します。
4. 必要に応じて、ドメインの名前と説明を変更し、保存を選択します。

音声プロファイルドメインの削除

誰が作成したかにかかわらず、任意の音声プロファイルドメインを削除できます。

> **Important**
>
> ドメインを削除すると、そのすべての音声プロファイルも削除され、削除を元に戻すことはできません。

音声プロファイルドメインを削除するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインで、音声プロファイルドメイン を選択します。
3. 削除するドメインの横にあるチェックボックスを選択し、削除を選択します。
4. 表示されるダイアログボックスで、このアクションを元に戻すことができないことを理解し、削除を選択します。

音声プロファイルドメインでのタグの使用

このセクションのトピックでは、既存の Amazon Chime SDK 音声プロファイルドメインでタグを使用する方法について説明します。タグを使用すると、ドメインにメタデータを割り当てることができます。タグは、リソースに関する情報、またはそのリソースに保持されているデータを保存するキーとオプションの値で構成されます。すべてのキーと値を定義します。例えば、 という名前のタグキーを 98765 の値CostCenterで作成し、 ペアをコスト配分に使用できます。音声プロファイルドメインには最大 50 個のタグを追加できます。

音声プロファイルドメインへのタグの追加

既存の音声プロファイルドメインにタグを追加するには、次の手順に従います。

タグを追加するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインで、音声プロファイルドメイン を選択します。
3. タグを追加するドメインを選択します。
4. タグの管理 を選択し、新しいタグの追加 を選択します。
5. キーボックスに値を入力し、値ボックスにオプションの値を入力します。
6. 必要に応じて、新しいタグを追加を選択して別のタグを作成します。
7. 完了したら、[変更を保存] を選択します。

音声プロファイルドメインタグの編集

必要なアクセス許可がある場合は、誰がタグを作成したかにかかわらず、AWSアカウント内の任意のタグを編集できます。ただし、IAM ポリシーでは、これを行うことができない場合があります。

タグを編集するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインで、音声プロファイルドメインを選択します。
3. 編集するタグがあるドメインを選択します。
4. [Manage tags (タグの管理)] を選択します。
5. 必要に応じて、キーボックスと値ボックスの値を変更します。

   -もしくは-

   新しいタグを追加を選択し、1 つ以上のタグを追加します。
6. 完了したら、[変更を保存] を選択します。

音声プロファイルドメインタグの削除

必要なアクセス許可がある場合は、誰がタグを作成したかにかかわらず、AWSアカウント内のタグを削除できます。ただし、IAM ポリシーでは、これを行うことができない場合があります。

タグを削除するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインで、音声プロファイルドメインを選択します。
3. 編集するタグがあるドメインを選択します。
4. [Manage tags (タグの管理)] を選択します。
5. 削除する各タグで 削除を選択します。
6. 完了したら、[変更を保存] を選択します。

音声分析の同意通知について

音声分析を使用する音声プロファイルドメインまたは通話分析設定を作成すると、次の同意確認が表示されます。

この機能を使用する条件として、発話者の生体認証識別子と生体認証情報 (「二項データ」) をデジタル埋め込み形式で収集、使用、保存、保持するには、文書によるリリースを含め、発話者の情報に基づいた同意が必要になる場合があることを承認します。このような同意は、イリノイ州、テキサス州、ワシントン州の生体認証法やその他の州のプライバシー法など、さまざまな州法で義務付けられています。発話者検索を使用する前に、適用法の義務に従い、この機能の使用に適用される当社のサービス条件に規定されたとおり、各発話者に必要なすべての通知を提供し、必要なすべての同意を取得する必要があります。

Amazon Chime SDK 音声分析サービスを使用する前に、サービスの使用を規定する AWS との契約の条項に従って、各発信者の同意を明確に反映したプロセスを通じて、各発信者に文書によるリリースを提供する必要があります。

イリノイ州の各話者については、生体情報プライバシー法 (BIPA) で規定されているように、話者検索を使用する前に、各発信者の情報に基づく同意を明確に反映したプロセスを通じて、書かれたリリースとして以下の情報を提供する必要があります。

「〔会社名 (「会社」)] は、音声検索サービスのサービスプロバイダーとして Amazon Web Services を使用します。発信者の音声を以前に保存した音声データと比較する目的で、Amazon Web

Services が [会社] に代わって、生体認証識別子と生体認証情報 (「生体認証データ」) を収集、保存、使用できます。このプロセスの一部として生成された対称データは、〔会社] との最後のやり取りから最大 3 年間保持されます。または、適用される法令で許可または要求され、その後破棄された場合のみ保持されます。適用される法令により要求または許可されている場合を除き、〔会社] は、そのようなデータの収集または取得の初期目的が満たされたとき、またはサービスとの最後のやり取り後 3 年以内、または当該データを破棄する必要があるとユーザーから通知された後のいずれか早い方に、〔会社] に保存された生体認証データを永続的に破棄するよう Amazon Web Services に指示します。対称データは、このサービスを提供および受信するために、必要に応じて [会社] と Amazon Web Services の間で送信される場合があります。お客様は、 [会社] と Amazon Web Services が、記載したとおりに生体認証データを収集、使用、および保存するにあたり、お客様の表現、通知、文書によるリリース、同意を提供します。」

以下のチェックボックスをオンにすると、BIPA の要求に応じて、イリノイの各発話者に対して、書き込み時に前述の情報を提供し、実行された書き込みリリースを取得することに同意したことになります。

緊急通報の設定

Amazon Chime SDK には、緊急通報を設定する 2 つの方法があります。どちらの方法も、 または米国で行われた呼び出しにのみ適用されます。

- 検証済みアドレス – 呼び出し元の住所を入力して検証します。このオプションを選択すると、検証済みの住所がすべての Amazon Chime SDK Voice Connector で利用可能になります。次に、Amazon Chime SDK は、最も近い Public safety Answering Point に通話をルーティングします。
- サードパーティールーティング – Amazon Chime SDK Voice Connector に緊急通報ルーティング番号を追加します。このオプションを選択すると、選択したサードパーティーサービスが通話をルーティングするため、住所を検証する必要はありません。この方法を使用して、米国外から緊急通報を行うことができますが、通話は米国のエンドポイントに送信する必要があります。

> **Note**
>
> アドレスまたはルーティング番号を使用しない場合、アドレス検証は 911 呼び出しの開始時に実行して、適切な Public safety Answering Point (PSAP) にルーティングされるようにすることができます。つまり、到着するまでに時間がかかる場合があります。

以下のセクションでは、両方のオプションを使用する方法について説明します。

トピック

緊急通報の住所の検証

緊急通報に住所を構築するには、通話の発信元となる住所を入力して検証します。次に、Amazon Chime SDK は、最も近いローカルの Public safety Answering Point (PSAP) に呼び出しをルーティングします。次の点に注意してください。

- アドレスの検証は 1 回のみ必要ですが、複数回検証できます。

- 建物の住所のみを検証します。スイート番号やアパート番号は含めないでください。
- 検証できるのは、米国の住所のみです。

> **Note**
>
> SIP リクエストの PIDF-LO オブジェクトで検証済みアドレスを使用することを強くお勧めします。詳細については、「緊急通報での PIDF-LO の使用」を参照してください。

アドレスを検証するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの [Phone Numbers] で、[Emergency Calling] をクリックします。
3. でValidate Address、建物の住所を入力します。

   > **Note**
   >
   > SIP 招待に表示されるとおりに住所を入力します。これにより、誰かが電話をかけるとアドレスが認識されます。

4. [Validate] を選択します。

サードパーティー緊急ルーティング番号の設定

緊急通報ルーティング番号を使用するには、以下が必要です。

- Amazon Chime SDK Voice Connector。
- サードパーティーサービスプロバイダーからの緊急通報ルーティング番号。これは米国の番号である必要があり、その番号を Amazon Chime SDK に提供します。緊急通報専用の Amazon Chime SDK Voice Connector を作成できます。

セットアップ後、緊急サービスに電話をかけると、Amazon Chime SDK は緊急番号を使用して、公衆交換電話ネットワーク経由でサードパーティー緊急サービスプロバイダーに通話をルーティングします。サードパーティー緊急サービスプロバイダーは、電話を緊急サービスにルーティングします。

米国内以外で緊急通報ルーティング番号を設定するには、以下の前提条件を満たす必要があります。

- サードパーティー緊急サービスプロバイダーから緊急通報ルーティング番号を取得します。米国の番号であることを確認してください。
- Voice Connector の終了と発信の設定をオンにして設定します。これを行うには、「」を参照してくださいAmazon Chime SDK Voice Connector 設定の編集。

Voice Connector の緊急通報ルーティング番号を設定するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの SIP Trunking で、音声コネクタ を選択します。
3. Voice Connector の名前を選択します。
4. 緊急呼び出しタブを選択します。
5. サードパーティー緊急サービスプロバイダー設定 で、 を追加 を選択します。
6. [Call send method] (通話送信方法) で、DNIS (ダイヤル番号識別サービス) を選択します。
7. [Emergency call routing number for calling emergency services] (緊急サービスを呼び出すための緊急通報ルーティング番号) に、緊急サービスを呼び出すためのサードパーティー電話番号を E.164 形式で入力します。
8. [Test routing number for calling emergency services] (緊急サービスを呼び出すためのテストルーティング番号) に、緊急サービスをテスト用に呼び出すためのサードパーティー電話番号を E.164 形式で入力します。
9. [Country] (国) を選択し、[United States] (米国) を選択します。
10. [追加] を選択します。

緊急通報での PIDF-LO の使用

Amazon Chime SDK Voice Connector は、拡張 911 (E911) 通話をサポートしています。Voice Connector を介して緊急通報を行うと、GEOPRIV Presence Information Data Format Location Object (PIDF-LO) を SIP リクエストに含めることで、発信者の位置情報を送信できます。オブジェクトには、 `Geolocation-Routing`ヘッダーを含めて、 に設定する必要がありますYes。アドレスを検証することを強くお勧めします。アドレスまたはルーティング番号を使用しない場合、アドレス検証は 911 呼び出しの開始時に実行して、適切な Public safety Answering Point (PSAP) にルーティングされるようにすることができます。つまり、到着するまでに時間がかかる場合があります。

次の例は、アドレスを含む PIDF-LO オブジェクトを含む SIP 招待を示しています。

```
INVITE sip:911@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws;transport=TCP SIP/2.0
Via: SIP/2.0/TCP IPaddress:12345;rport;branch=z9hG4bKKXN2D41yvDUKH
From: +15105186683 ><sip:+15105186683@IPaddress:12345>;tag=tag
To: <sip:911@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws>;transport=TCP
Call-ID: 12abcdef-3456-7891-012g-h7i8j9k6l0a1
CSeq: 43615607 INVITE
Contact: <sip:IPaddress:12345>
Max-Forwards: 70
Geolocation-Routing: Yes
Geolocation: <cid:a1ef610291734f98a467b973819e90ed>;inserted-by=vpc@ng911.test.com
Content-Type: multipart/mixed;boundary=unique-boundarystring
Content-Length: 271
Accept: application/sdp, application/pidf+xml

--unique-boundarystring
Content-Type: application/sdp
v=0
o=FreeSWITCH 1636327400 1636327401 IN IP4 IPaddress
s=FreeSWITCH
c=IN IP4 IPaddress
t=0 0
m=audio 11398 RTP/SAVP 9 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=sendrecv
a=ptime:20

--unique-boundarystring
Content-Type: application/pidf+xml
Content-ID: <pidftest@test.com>
<?xml version="1.0" encoding="utf-8"?>
<presence xmlns="urn:ietf:params:xml:ns:pidf"
xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
xmlns:bp="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy"
xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
entity="sip:amazontest911@test.com">
<tuple id="0">
    <status>
    <gp:geopriv>
        <gp:location-info>
        <ca:civicAddress>
```

```
            <ca:country>US</ca:country>
            <ca:A1>WA</ca:A1>
            <ca:A3>Seattle</ca:A3>
            <ca:HNO>1812</ca:HNO>
            <ca:RD>Example</ca:RD>
            <ca:STS>Ave</ca:STS>
            <ca:NAM>Low Flying Turtle</ca:NAM>
            <ca:PC>98101</ca:PC>
        </ca:civicAddress>
        </gp:location-info>
    </gp:geopriv>
    </status>
    <timestamp>2021-09-22T13:37:31.03</timestamp>
</tuple>
</presence>
--unique-boundarystring--
```

SIP メディアアプリケーションの管理

Amazon Chime SDK コンソールを使用して、セッション開始プロトコル (SIP) メディアアプリケーションを作成できます。SIP メディアアプリケーションを使用すると、通常は構内交換機 (PBX) に基づいて構築されるカスタム信号やメディア命令を簡単かつ迅速に作成できます。

また、 コンソールを使用して SIP ルールを作成します。SIP ルールは、SIP メディアアプリケーションが Amazon Chime SDK 会議に接続する方法を指定します。通話は、Amazon Chime SDK インベントリからプロビジョニングされたパブリック DID または通話料無料の電話番号との間で送受信できます。または、Amazon Chime SDK Voice Connector に割り当てられた名前であるリクエスト URI ホスト名との間で送受信できます。Amazon Chime SDK は、ユーザーが電話に出たとき、または通話を受信したときに SIP ルールを実行します。SIP ルールの使用については、「」を参照してくださいSIP ルールの管理。

SIP メディアアプリケーションを作成するには、AWS Lambda ユーザーでなければなりません。SIP メディアアプリケーションは、以下の理由で Lambda 関数を使用します。

- 意思決定を伴う複雑なロジックを書くことができます。例えば、発信者はタッチトーン電話を使用して会議にダイヤルインできます。今度は、その電話番号がトリガーする Lambda 関数が会議 PIN を要求し、発信者を正しい会議に誘導します。
- サーバーインフラストラクチャなしで Lambda 関数をデプロイできます。

AWS Lambda の詳細については「AWS Lambda の使用開始」を参照してください。

> **Note**
>
> Amazon Chime SDK SIP メディアアプリケーションには、アウトバウンドの国際通話制限があります。詳細については、「発信通話の制限」を参照してください。

トピック

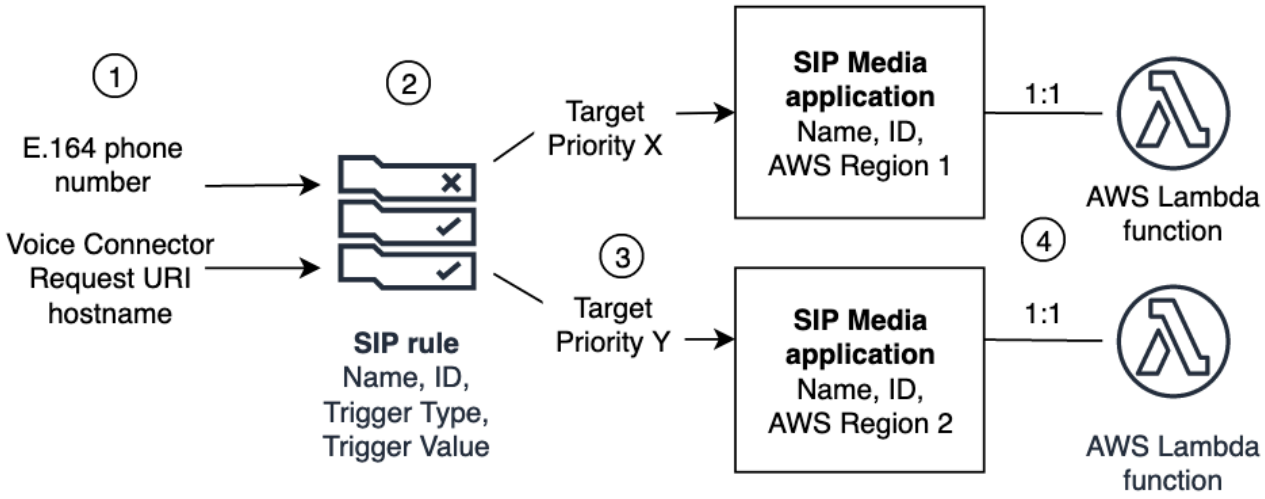
- SIP アプリケーションとルールについて
- SIP メディアアプリケーションの使用

SIP アプリケーションとルールについて

Amazon Chime SDK でセッション開始プロトコル (SIP) を使用するには、SIP メディアアプリケーションと SIP ルールを作成します。両方を Amazon Chime SDK コンソールで作成します。

次の図は、アプリケーションとルールの仕組みを示しています。これは SIP ルールによって電話番号とリクエスト URI のホスト名から異なる SIP アプリケーションに通話がルーティングされるしくみを示しています。

画像の数字は、画像の下のテキスト内の数字に対応しています。



Chime インベントリと Voice Connector (1) の電話番号は、SIP ルール (2) にのみ割り当てることができます。また、PSTN Audio サービスで電話番号または Amazon Chime SDK Voice Connector をプロビジョニングする必要があります。その手順については、「」でSIP メディアアプリケーションの作成説明します。電話番号への通話を受信すると、SIP ルールは SIP メディアアプリケーションとそれに関連する Lambda 関数を呼び出します (4)。Lambda 関数は、保留時の音楽の再生、会議への参加、通話のミュートなどのアクションを呼び出すコードを実行します。マルチリージョンの耐障害性を提供するために、SIP ルール (2) では、フェイルオーバーの優先順位に従って、異なるAWS リージョン (3) の代替ターゲット SIP メディアアプリケーションを指定できます。1 つのターゲットに障害が発生した場合、PSTN Audio サービスは次のターゲットを試行します。代替ターゲットはそれぞれ異なる AWS リージョンに存在していなければならない点に注意してください。

SIP メディアアプリケーションの使用

SIP メディアアプリケーションは、SIP ルールからターゲットAWS Lambda関数に値を渡すマネージドオブジェクトです。SIP メディアアプリケーションを作成、表示、更新、および削除できます。任意のアプリケーションの詳細を表示できますが、それらのアプリケーションを自分以外の管理者も表示できる点に注意してください。

> **Note**
>
> SIP メディアアプリケーションを作成するには AWS Lambda 関数が必要です。詳細については「AWS Lambda の使用開始」を参照してください。

トピック

SIP メディアアプリケーションの作成

SIP メディアアプリケーションは、リクエスト URI ホスト名、Amazon Chime SDK Voice Connector グループ、またはプライベート電話番号との間の通話を有効にする必要がある場合に作成します。

SIP メディアアプリケーションを作成するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの PSTN Audio で SIP メディアアプリケーション を選択し、表示されるページで SIP メディアアプリケーションの作成 を選択します。
3. 名前 に、アプリケーションの名前を入力します。
4. 次のいずれかの値をコピーし、ARN ボックスに貼り付けます。

- Lambda 関数の ARN
- Lambda 関数のエイリアスの ARN
- Lambda 関数のバージョン ARN

> **Note**
>
> Lambda 関数を構築するときにエイリアスとバージョン ARNs を作成できます。Lambda 同時実行を有効にする場合は、エイリアスまたはバージョン ARN が必要です。Lambda 関数のエイリアス、バージョンエイリアス、および同時実行の詳細については、「 AWS Lambdaデベロッパーガイド」の「Lambda 関数のエイリアス」、「Lambda 関数のバージョン」、および「Lambda プロビジョニング済み同時実行数の管理」を参照してください。

5. (オプション) タグ で、新しいタグ を追加 を選択し、次の操作を行います。

   1. キーボックスに値を入力します。
   2. (オプション) 値 ボックスに値を入力します。
   3. 必要に応じて、新しいタグを追加を選択してさらにタグを追加します。

6. SIP メディアアプリケーションの作成を選択します。

   [Create a SIP media application] (SIP メディアアプリケーションの作成) ページの最上部に成功メッセージが表示され、アプリケーションのリストに作成されたメディアアプリケーションが表示されます。エラーメッセージが表示された場合、その指示に従ってください。

SIP メディアアプリケーションでのタグの使用

このセクションのトピックでは、既存の Amazon Chime SDK SIP メディアアプリケーションでタグを使用する方法について説明します。タグを使用すると、SIP メディアアプリケーションなどのAWSリソースにメタデータを割り当てることができます。タグは、リソースに関する情報、またはそのリソースに保持されているデータを保存するキーとオプションの値で構成されます。すべてのキーと値を定義します。例えば、 という名前のタグキーを の値`CostCenter`で作成`98765`し、そのペアをコスト配分に使用できます。SIP メディアアプリケーションには最大 50 個のタグを追加できます。

トピック

- SIP メディアアプリケーションへのタグの追加

- タグの編集
- タグの削除

SIP メディアアプリケーションへのタグの追加

既存の Amazon Chime SDK SIP メディアアプリケーションには、最大 50 個のタグを追加できます。

タグを追加するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの PSTN Audio で、SIP メディアアプリケーション を選択します。
3. 使用する SIP メディアアプリケーションの名前を選択します。
4. [タグ] タブ、[タグを管理] の順に選択します。
5. 新しいタグを追加を選択し、キーとオプションの値を入力します。
6. 必要に応じて、新しいタグを追加を選択して別のタグを作成します。
7. 完了したら、[変更を保存] を選択します。

タグの編集

必要なアクセス許可がある場合は、誰がタグを作成したかにかかわらず、AWSアカウント内の任意のタグを編集できます。ただし、IAM ポリシーでは、これを行うことができない場合があります。

タグを編集するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの PSTN Audio で、SIP メディアアプリケーション を選択します。
3. 変更する SIP メディアアプリケーションの名前を選択します。
4. [タグ] タブ、[タグを管理] の順に選択します。
5. キーまたは値 ボックスに新しい値を入力します。
6. 完了したら、[変更を保存] を選択します。

タグの削除

必要なアクセス許可がある場合は、誰がタグを作成したかにかかわらず、AWSアカウント内のタグを削除できます。ただし、IAM ポリシーでは、これを行うことができない場合があります。

タグを削除するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの PSTN Audio で、SIP メディアアプリケーション を選択します。
3. 変更する SIP メディアアプリケーションの名前を選択します。
4. [タグ] タブ、[タグを管理] の順に選択します。
5. 削除するタグの横にある 削除を選択します。
6. [変更の保存] をクリックします。

SIP メディアアプリケーションの表示

自分の SIP メディアアプリケーションを他の管理者が詳細まで表示でき、自分は他の管理者のアプリケーションを詳細まで表示できます。

SIP メディアアプリケーションを表示するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインで、[SIP media applications] (SIP メディアアプリケーション) を選択します。

   [SIP media application] (SIP メディアアプリケーション) ページに組織内のすべてのアプリケーションが表示されます。
3. アプリケーションの詳細を表示するには、アプリケーションの名前を選択します。

SIP メディアアプリケーションの更新

SIP メディアアプリケーションの Lambda 関数の名前と Amazon リソースネーム (ARNsを更新できます。AWS リージョンを更新することはできません。

SIP メディアアプリケーションを更新するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインで、[SIP media applications] (SIP メディアアプリケーション) を選択します。

   [SIP media application] (SIP メディアアプリケーション) ページが表示されます。
3. 更新したいアプリケーションの名前を選択します。

   アプリケーションは固有のページに表示されます。
4. [編集] を選択します。
5. 必要に応じて、以下を変更します。

   - アプリケーションの名前
   - Lambda ARN、エイリアス ARN、またはバージョン ARN
   - タグ。タグの変更の詳細については、「」を参照してください。

   > **Note**
   >
   > Lambda 関数を構築するときにエイリアスとバージョン ARNs を作成できます。Lambda 同時実行を有効にする場合は、エイリアスまたはバージョン ARN が必要です。Lambda 関数のエイリアス、バージョンエイリアス、および同時実行の詳細については、「 AWS Lambdaデベロッパーガイド」の「Lambda 関数のエイリアス」、「Lambda 関数のバージョン」、および「Lambda プロビジョニング済み同時実行数の管理」を参照してください。
6. [Save] (保存) を選択します。

   成功メッセージが表示されます。エラーメッセージが表示された場合、その指示に従ってください。

SIP メディアアプリケーションの削除

SIP メディアアプリケーションを削除したい理由としてはいくつかがあり、次のような例が挙げられます。

- 電話番号またはリクエスト URI のホスト名の使用を停止します。
- SIP メディアアプリケーションの作成が間違っています。

> **Note**
>
> ベストプラクティスとして、アプリケーションを削除しても通話の流れが中断されないことを確認します。また、アプリケーションを削除しても、関連する電話番号や SIP ルールは削除されません。

SIP メディアアプリケーションを削除するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインで、[SIP media applications] (SIP メディアアプリケーション) を選択します。

   [SIP media application] (SIP メディアアプリケーション) ページが表示されます。
3. アプリケーション名の隣にあるオプションボタンを選択します。
4. [削除] をクリックします。

   [Delete application name] (アプリケーション名の削除) ダイアログボックスが表示されます。
5. [I understand that this action cannot be reversed] (この処理は元に戻せないことを理解しています) を選択してから [Delete] (削除) を選択します。

Amazon Chime SDK Alexa スキル呼び出しの有効化

Alexa スキルを作成する場合は、 StartCommunicationSession API を使用して、それらのスキルから直接 を呼び出すことができます。呼び出しを有効にするには、以下を実行する必要があります。

- Alexa デベロッパーコンソールを使用してスキルのクライアント ID を検索します。
- Amazon Chime SDK コンソールを使用して、少なくとも 1 つの SIP メディアアプリケーションのスキル呼び出しを有効にします。
- Alexa デベロッパーコンソールを再度使用して、スキルのコミュニケーション - 呼び出しのアクセス許可を有効にします。

以下のトピックでは、これらのタスクを完了する方法について説明します。記載されている順序に従ってください。これらを完了したら、「Amazon Chime SDK デベロッパーガイド」の「Amazon Chime SDK Alexa スキル呼び出しの使用」を参照して、Alexa スキルにスキル呼び出しを追加する方法を確認してください。

1: スキルのクライアント ID を検索する

Alexa スキルと Amazon Chime SDK SIP メディアアプリケーションを統合するには、まずスキルのクライアント ID を見つける必要があります。

> **Note**
>
> Alexa スキルにはスキル IDsとクライアント IDs。これらのステップでは、クライアント ID のみを使用します。

スキルのクライアント ID を検索するには

1. Alexa デベロッパーコンソール で、目的のスキルを選択します。
2. 「ツール」を選択し、「アクセス許可」を選択します。
3. ページの下部にある Timers を選択して Timers アクセス許可を有効にし、Timers を選択して Timers アクセス許可を無効にします。

   クライアント ID はアクセス許可ページの下部に表示されます。ID のプレフィックスは で、その後に文字列がamzn1.application-oa2-client続きます。例えば、amzn1.application-oa2-client.ad213256-e602-4756-9534-cc3b76b670b4 です。
4. その ID をコピーして、次のステップに進みます。

2: スキルと SIP メディアアプリケーションを統合する

スキルのクライアント ID が見つかったら、それを使用してスキルと SIP メディアアプリケーションを統合します。

Alexa を SIP メディアアプリケーションと統合するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。

2. ナビゲーションペインの SIP トランキング で、SIP メディアアプリケーション を選択します。
3. 統合する SIP メディアアプリケーションを選択します。
4. Alexa スキル設定タブを選択します。
5. Alexa スキルステータス で、有効ボタンを選択します。
6. Alexa スキルクライアント ID で、前のステップの ID を入力します。
7. [Save] (保存) を選択します。

3. コミュニケーションを有効にする - スキルの呼び出し許可

スキルと SIP メディアアプリケーションを統合したら、Alexa デベロッパーコンソールを使用して、スキルのコミュニケーション - 通話許可を有効にします。デフォルトでは、このアクセス許可はスキルと SIP メディアアプリケーションを統合する後にのみ表示されます。これを行うと、Alexa デベロッパーコンソールのアクセス許可ページの下部に、Communication - Calling アクセス許可が表示されます。

アクセス許可を有効にすると、スキルはユーザーに通話を行う同意を求めます。

アクセス許可を有効にするには

1. Alexa デベロッパーコンソール で、目的のスキルを選択します。
2. 「ツール」を選択し、「アクセス許可」を選択します。
3. ページの下部で、Communication - Calling スライダーをオンの位置に移動します。

SIP ルールの管理

SIP ルールは、SIP メディアアプリケーションを電話番号またはリクエスト URI のホスト名に関連付けます。1 つの SIP ルールを複数の SIP メディアアプリケーションに関連付けることができます。その後、各アプリケーションでそのルールのみが実行されます。SIP ルールが SIP メディアアプリケーションと連携する方法の概要については、前のセクションSIP アプリケーションとルールについての「」を参照してください。

> **Note**
>
> SIP ルールを作成するには、Amazon Chime SDK インベントリで製品タイプが SIP メディアアプリケーションダイヤルインに設定されている DID または通話料無料電話番号、または Amazon Chime SDK Voice Connector に割り当てられた名前であるリクエスト URI ホスト名が少なくとも 1 つ必要です。電話番号の詳細については、「電話番号の管理」を参照してください。リクエスト URI ホスト名の詳細については、次のセクションの手順に従ってください。

目次

SIP ルールの作成

SIP ルールを作成する前に、Amazon Chime SDK インベントリで製品タイプが SIP メディアアプリケーションダイヤルインに設定されている DID または通話料無料電話番号、または Amazon Chime SDK Voice Connector に関連付けられたリクエスト URI ホスト名、および SIP メディアアプリケーションが必要です。SIP アプリケーションの詳細については、「SIP メディアアプリケーションの作成」を参照してください。また、他の管理者が作成したルールを使用することもできます。

SIP ルールを作成するには:

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの電話番号 で、SIP メディアアプリケーション を選択します。
3. ルールを作成する SIP アプリケーションを選択し、ルールタブを選択します。
4. 電話番号またはアウトバウンドホスト名の値をコピーし、その値をメモ帳または同様のプログラムに貼り付け、後で使用するためにプログラムを開いたままにします。
5. ナビゲーションペインで [SIP rules] (SIP ルール) を選択します。

   [SIP rules] (SIP ルール) ページが表示されます。
6. [作成] を選択します。

   [Create a SIP rule] (SIP ルールを作成する) ダイアログボックスが表示されます。
7. 名前 ボックスにルールの名前を入力し、次のいずれかを実行します。

   電話番号のルールを作成する

   A. デフォルトでは、[Trigger type] (トリガータイプ) リストに [To phone number] (電話番号へ) が表示されます。表示されない場合、リストでその値を選択します。

   B. [Phone number] (電話番号) で、電話番号を入力するか、またはリストから電話番号を選択します。番号を入力する場合、**+1***10 ####*を入力します。例: +15095551212

   リクエスト URI ホスト名のルールを作成する

   A. [Trigger type] (トリガータイプ) リストを開いて [Request URI hostname] (リクエスト URI のホスト名) を選択します。

   B. ステップ 2 でコピーしたホスト名を [Request URI hostname] (リクエスト URI のホスト名) フィールドに貼り付けます。
8. ルールを直ちに使用するには、 [Enabled] (有効) チェックボックスをオンのままにします。Amazon Chime SDK Voice Connector とそのホスト名が利用可能になるまで、ルールを無効にするには、このチェックボックスをオフにします。
9. 次へを選択し、ステップ 2 ページで SIP メディアアプリケーションリストを開き、使用する SIP メディアアプリケーションを選択します。
10. 必要に応じて、[Add a SIP media application] (SIP メディアアプリケーションの追加) を選択すると複数のアプリケーションでルールを使用できます。

11. [作成] を選択します。

    成功メッセージが表示されます。エラーメッセージが表示された場合、指示に従ってください。

SIP ルールの表示

自分の SIP ルールを他の管理者が詳細まで表示でき、自分は他の管理者のルールを詳細まで表示できます。

SIP ルールを表示するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの PSTN Audio で、SIP ルール を選択します。

   [SIP rules] (SIP ルール) ページに組織内のすべてのルールが表示されます。
3. ルールの詳細を表示するには、ルールの名前を選択します。

SIP ルールの更新

SIP ルールについてできる唯一の更新は、名前を変更することです。通常、ルール名を変更する場合には、対応する SIP メディアアプリケーションの名前と一致するようにしてください。

SIP ルールを更新するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの PSTN Audio で SIP ルール を選択します。
3. 変更したいルールの名前を選択します。

   そのルールのページが表示されます。
4. [編集] を選択します。
5. ルールに付ける新しい名前を [Name] (名前) に入力して [Save] (保存) を選択します。

SIP ルールの有効化

別の管理者によって作成されたルールも含め、任意の SIP ルールを有効にできます。ベストプラクティスとして、ルールの詳細を確認してから有効にします。詳細については、「SIP ルールの表示」を参照してください。

SIP ルールを有効にするには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの PSTN Audio で SIP ルール を選択します。

   [SIP rules] (SIP ルール) ページが表示されます。
3. 必要に応じて、ルールリストの末尾までスクロールしてから水平スクロールバーを使用して [Status] (ステータス) 列を表示します。

   無効になっているルールには赤色の [Disabled] (無効) アイコンが付きます。
4. ルールを有効にするには、次のいずれかの操作をします。

   アクションリストを使用する

   A. スクロールして、ルール名の隣にあるオプションボタンを選択します。

   B. 上にスクロールして、[Actions] (アクション) リストを開き、[Enable] (有効にする) を選択してからステップ 5 に進みます。

   Enable (有効にする) ボタンを使用する

   A. ルールの名前を選択します。

   B. [Edit] (編集) の隣にある [Enable] (有効にする) を選択してからステップ 5 に進みます。
5. ステップ 4 で説明したいずれかの方法を用いて [Enable] (有効にする) を選択した場合、[Enable rule(s)] (ルールの有効化) ダイアログボックスが表示されます。[I understand that the rule(s) listed here will trigger the SIP media application] (このリストに表示されたルールが SIP メディアアプリケーションをトリガーすることを理解しています) を選択してから [Enable] (有効にする) を選択します。

SIP ルールの無効化

ルールによる接続の必要がない場合、SIP ルールを無効にします。また、SIP ルールまたは関連する SIP メディアアプリケーションを削除する前に、その ルールを無効にする必要があります。管理者によって作成されたルールはどれでも無効にできます。ベストプラクティスとして、ルールを無効にする前にルールの詳細を表示し、ルールを無効にしても通話の流れが中断されないことを確認します。詳細については、「SIP ルールの表示」を参照してください。

SIP ルールを無効にするには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの PSTN Audio で SIP ルール を選択します。

   [SIP rules] (SIP ルール) ページが表示されます。
3. 必要に応じて、ルールリストの末尾までスクロールしてから水平スクロールバーを使用して [Status] (ステータス) 列を表示します。

   有効なルールには緑色の [Enabled] (有効) アイコンが付きます。
4. ルールを無効にするには、次のいずれかの操作をします。

   アクションリストを使用する

   A. スクロールして、ルール名の隣にあるオプションボタンを選択します。

   B. 上にスクロールして、[Actions] (アクション) リストを開いて [Disable] (無効にする) を選択します。

      [Disable rule(s)] (ルールの無効化) ダイアログボックスが表示されます。ステップ 5 に進みます。

   [Disable] (無効にする) ボタンを使用する

   A. スクロールして、ルールの名前を選択します。

   B. [Edit] (編集) の隣にある [Disable] (無効にする) を選択します。

      [Disable rule(s)] (ルールの無効化) ダイアログボックスが表示されます。ステップ 5 に進みます。

5. このアクションによって SIP メディアアプリケーション をトリガーする上記のルールが停止されることを理解し、 を無効にするを選択します。

SIP ルールの削除

通常、関連付けられたリクエスト URI のホスト名または電話番号が不要になった場合、SIP ルールを削除します。間違って作成した SIP ルールを削除することもできます。

> **Note**
>
> ルールを削除する前に、まずそれを無効にする必要があります。ルールの無効化の詳細については、「SIP ルールの無効化」を参照してください。

SIP ルールを削除するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの PSTN Audio で SIP ルール を選択します。

   [SIP rules] (SIP ルール) ページが表示されます。
3. ルール名の横にあるラジオボタンを選択します。
4. [Actions] (アクション) リストを開いて [Delete] (削除) を選択します。

   [Delete rule(s)] (ルールの削除) ダイアログボックスが表示されます。
5. [I understand that this action cannot be reversed] (この処理は元に戻せないことを理解しています) を選択してから [Delete] (削除) を選択します。

Amazon Chime SDK のグローバル設定の管理

Amazon Chime SDK の通話詳細レコード設定を管理します。

通話詳細レコードの設定

Amazon Chime SDK 管理アカウントの通話詳細レコード設定を構成する前に、まず Amazon Simple Storage Service バケットを作成する必要があります。Amazon S3 バケットは、通話詳細レコードのログ記録先として使用されます。通話詳細レコード設定を構成するときは、データを保存および管理するために、Amazon Chime SDK に Amazon S3 バケットへの読み取りおよび書き込みアクセスを許可します。Amazon S3 バケットの作成方法の詳細については、Amazon Simple Storage Service ユーザーガイドの「Amazon Simple Storage Service の開始方法」を参照してください。

Amazon Chime SDK Voice Connector の通話詳細レコード設定を構成できます。Amazon Chime SDK Voice Connector の詳細については、「」を参照してくださいAmazon Chime SDK での電話番号の管理。

通話詳細レコード設定を構成するには

1. Amazon Simple Storage Service ユーザーガイドの「Amazon Simple Storage Service の開始方法」の手順に従って Amazon S3 バケットを作成します。
2. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
3. ナビゲーションペインの SIP Trunking で、通話詳細レコード を選択します。
4. ログ送信先リストを開き、S3 バケットを選択します。
5. [Save] (保存) を選択します。

通話詳細レコードのログ記録はいつでも停止できます。

通話詳細レコードのログ記録を停止するには

1. https://console.aws.amazon.com/chime-sdk/home で Amazon Chime SDK コンソールを開きます。
2. ナビゲーションペインの SIP Trunking で、通話詳細レコード を選択します。
3. ログ記録の無効化を選択します。

Amazon Chime SDK Voice Connector 通話詳細レコード

Amazon Chime SDK Voice Connector の通話詳細レコードを受信すると、Amazon S3 バケットに送信されます。次の例は、Amazon Chime SDK Voice Connector 通話詳細レコード名の一般的な形式を示しています。

```
Amazon-Chime-Voice-Connector-CDRs/
json/abcdef1ghij2klmno3pqr4/2019/03/01/17.10.00.020_123abc4d-efg5-6789-h012-
j3456789k012
```

次の例は、通話詳細レコード名で表されるデータを示しています。

```
Amazon-Chime-Voice-Connector-CDRs/json/voiceConnectorID/year/month/
day/callStartTime-voiceConnectorTransactionID
```

次の例は、Amazon Chime SDK Voice Connector 通話詳細レコードの一般的な形式を示しています。

```
{
    "AwsAccountId": "111122223333",
    "TransactionId": "123abc4d-efg5-6789-h012-j3456789k012",
    "CallId": "123a4b567890123c456789012d3456e7@203.0.113.9:8080",
    "VoiceConnectorId": "abcdef1ghij2klmno3pqr4",
    "Status": "Completed",
    "StatusMessage": "OK",
    "SipAuthUser": "XXXX",
    "BillableDurationSeconds": 6,
    "BillableDurationMinutes": 0.1,
    "SchemaVersion": "2.0",
    "SourcePhoneNumber": "+12065550100",
    "SourcePhoneNumberName": "North Campus Reception",
    "SourceCountry": "US",
    "DestinationPhoneNumber": "+12065550101",
    "DestinationPhoneNumberName": "South Campus Reception",
    "DestinationCountry": "US",
    "UsageType": "USE1-US-US-outbound-minutes",
    "ServiceCode": "AmazonChimeVoiceConnector",
    "Direction": "Outbound",
    "StartTimeEpochSeconds": 1565399625,
    "EndTimeEpochSeconds": 1565399629,
    "Region": "us-east-1",
```

```
    "Streaming": true
}
```

Amazon Chime SDK Voice Connector ストリーミング詳細レコード

Amazon Chime SDK Voice Connector の通話詳細レコードを受信することを選択し、Kinesis Video Streams にメディアをストリーミングするか、SIPREC リクエストを送信すると、ストリーミング詳細レコードが Amazon S3 バケットに送信されます。詳細については、「Amazon Chime SDK Voice Connector メディアを Kinesis にストリーミングする」を参照してください。

次の例は、ストリーミング詳細レコード名の一般形式を示しています。

```
Amazon-Chime-Voice-Connector-SDRs/
json/abcdef1ghij2klmno3pqr4/2019/03/01/17.10.00.020_123abc4d-efg5-6789-h012-
j3456789k012
```

次の例は、ストリーミング詳細レコード名で表されるデータを示しています。

```
Amazon-Chime-Voice-Connector-SDRs/json/voiceConnectorID/year/month/
day/callStartTime-voiceConnectorTransactionID
```

次の例は、ストリーミング詳細レコードの一般形式を示しています。

```
{
    "SchemaVersion": "1.0",
    "AwsAccountId": "111122223333",
    "TransactionId": "123abc4d-efg5-6789-h012-j3456789k012",
    "CallId": "123a4b567890123c456789012d3456e7@203.0.113.9:8080",
    "VoiceConnectorId": "abcdef1ghij2klmno3pqr4",
    "StartTimeEpochSeconds": 1565399625,
    "EndTimeEpochSeconds": 1565399629,
    "Status": "Completed",
    "StatusMessage": "Streaming succeeded",
    "ServiceCode": "AmazonChime",
    "UsageType": "USE1-VC-kinesis-audio-streaming",
    "BillableDurationSeconds": 6,
    "Region": "us-east-1"
}
```

ネットワーク設定と帯域幅の要件

Amazon Chime SDK では、さまざまな のサービスをサポートするために、このトピックで説明されている送信先とポートが必要です。インバウンドまたはアウトバウンドのトラフィックがブロックされていると、オーディオ、ビデオ、画面共有、チャットなどのさまざまなサービスに影響する場合があります。

Amazon Chime SDK は、ポート TCP/443 で Amazon Elastic Compute Cloud (Amazon EC2) およびその他の AWSサービスを使用します。ファイアウォールがポート TCP/443 をブロックする場合は、AWS 全般のリファレンス次のサービスの `*.amazonaws.com` を許可リストに入れるか、AWSIP アドレス範囲を に配置する必要があります。

- Amazon EC2
- Amazon CloudFront
- Amazon Route 53

共通

環境で Amazon Chime SDK を実行する場合は、次の宛先とポートが必要です。

デスティネーション	ポート
*.chime.aws	TCP: 443
*.amazonaws.com	TCP: 443

Amazon Chime SDK WebRTC メディアセッション

ドメイン	サブネット	ポート
*.chime.aws	99.77.128.0/18	TCP:443 UDP:3478
*.sdkassets.chime.aws		TCP: 443

Amazon Chime SDK Voice Connector

Amazon Chime SDK Voice Connector を使用する場合は、次の宛先とポートをお勧めします。

SIP シグナリング

AWS リージョン	デスティネーション	ポート
米国東部 (バージニア北部)	3.80.16.0/23	UDP/5060 TCP/5060 TLS/5061
米国西部 (オレゴン)	99.77.253.0/24	UDP/5060 TCP/5060 TLS/5061
アジアパシフィック (ソウル)	99.77.242.0/24	UDP/5060 TCP/5060 TLS/5061
アジアパシフィック (シンガポール)	99.77.240.0/24	UDP/5060 TCP/5060 TLS/5061
アジアパシフィック (シドニー)	99.77.239.0/24	UDP/5060 TCP/5060 TLS/5061
アジアパシフィック (東京)	99.77.244.0/24	UDP/5060 TCP/5060

AWS リージョン	デスティネーション	ポート
		TLS/5061
カナダ (中部)	99.77.233.0/24	UDP/5060 TCP/5060 TLS/5061
欧州 (フランクフルト)	99.77.247.0/24	UDP/5060 TCP/5060 TLS/5061
欧州 (アイルランド)	99.77.250.0/24	UDP/5060 TCP/5060 TLS/5061
欧州 (ロンドン)	99.77.249.0/24	UDP/5060 TCP/5060 TLS/5061

メディア

AWS リージョン	デスティネーション	ポート
アジアパシフィック (ソウル)	99.77.242.0/24	UDP/5000:65000
アジアパシフィック (シンガポール)	99.77.240.0/24	UDP/5000:65000
アジアパシフィック (シドニー)	99.77.239.0/24	UDP/5000:65000

AWS リージョン	デスティネーション	ポート
アジアパシフィック (東京)	99.77.244.0/24	UDP/5000:65000
カナダ (中部)	99.77.233.0/24	UDP/5000:65000
欧州 (フランクフルト)	99.77.247.0/24	UDP/5000:65000
欧州 (アイルランド)	99.77.250.0/24	UDP/5000:65000
欧州 (ロンドン)	99.77.249.0/24	UDP/5000:65000
米国東部 (バージニア北部)	3.80.16.0/23	UDP/5000:65000
米国東部 (バージニア北部)	52.55.62.128/25	UDP/1024:65535
米国東部 (バージニア北部)	52.55.63.0/25	UDP/1024:65535
米国東部 (バージニア北部)	34.212.95.128/25	UDP/1024:65535
米国東部 (バージニア北部)	34.223.21.0/25	UDP/1024:65535
米国西部 (オレゴン)	99.77.253.0/24	UDP/5000:65000

通信事業者のメディア送信先とポートの Amazon Voice Focus

AWS リージョン	デスティネーション	ポート
米国東部 (バージニア北部)	99.77.254.0/24	UDP/5000:65000
米国西部 (オレゴン)	99.77.232.0/24	UDP/5000:65000

帯域幅の要件

Amazon Chime SDK には、提供するメディアに対して次の帯域幅要件があります。

- 音声
  - 1:1 呼び出し: 54 kbps 上りおよび下り

  - 大規模な呼び出し: 発信者が 50 人の場合に 32 kbps を超えない
- 動画
  - 1:1 呼び出し: 650 kbps 上りおよび下り
  - HD モード :1400 kbps 上りおよび下り
  - 3 ~ 4 人: 450 kbps 上りおよび (N-1)*400 kbps 下り
  - 5 ~ 16 人: 184 kbps 上りおよび (N-1)*134 kbps 下り
  - 上下の帯域幅はネットワーク状況に応じて低くなります
- 画面
  - 1.2 mbps 上 (提示時) と下 (表示時) (高品質の場合)。これは、ネットワークの状態に基づいて 320 kbps まで下がります。
  - リモート制御: 800 kbps 固定

Amazon Chime SDK Voice Connector には、次の帯域幅要件があります。

- 音声
  - 通話: ~ 90 kbps 上下 メディアペイロードおよびパケットオーバーヘッドが含まれます。
- T.38 FAX
  - V.34 使用あり: ~ 40 kbps メディアペイロードおよびパケットオーバーヘッドが含まれます。
  - V.34 使用なし: ~ 20 kbps メディアペイロードおよびパケットオーバーヘッドが含まれます。

Amazon Chime SDK の管理サポート

管理者であり、Amazon Chime SDK のサポートに連絡する必要がある場合は、次のいずれかのオプションを選択します。

- AWS サポートのアカウントをお持ちの場合は、[サポートセンター] にアクセスし、チケットを送信します。
- それ以外の場合は、 を開き、Amazon Chime SDK、サポート、リクエストの送信 AWS Management Consoleを選択します。

次の情報を入力すると便利です。

- 問題についての詳しい説明。
- タイムゾーンを含む、問題が発生した時刻。

Amazon Chime SDK 管理ガイドのドキュメント履歴

次の表は、2022 年 3 月以降の「Amazon Chime SDK 管理ガイド」の重要な変更点をまとめたものです。このドキュメントの更新に関する通知を受け取るには、RSS フィードにサブスクライブしてください。

変更	説明	日付
サービスにリンクされたロールポリシーの更新	がサービスダッシュボードで使用するためのメトリクス CloudWatch を提供できるようにする、`AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy` 追加されたアクセス許可。詳細については、「Amazon Chime SDK メディアパイプラインでのロールの使用」および「AWS マネージドポリシー: AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy」を参照してください。	2023 年 12 月 8 日
サービスにリンクされたロールポリシーの更新、新しい会議リージョン	Kinesis Video Streams が Amazon Chime SDK 会議にオーディオ、ビデオ、および画面共有データをストリーミングできるようにするアクセス許可`AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy` が追加されました。詳細については、「Amazon Chime SDK メディアパイプラインでのロールの使用」およ	2023 年 9 月 25 日

	び「AWS マネージドポリシー：AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy」を参照してください。	
音声エンハンスメント	管理者は、通話を有効にすることで、音声の機能強化を有効にできるようになりました。これは、PSTN 通話の音声品質を向上させる機能です。詳細については、「通話分析設定の作成」の「音声の機能強化について」セクションを参照してください。	2023 年 8 月 31 日
サービスにリンクされたロールポリシーの更新	GetMediaInsightsPipelineConfiguration API へのアクセスを許可するAmazonChimeVoiceConnectorServiceLinkedRolePolicy 追加アクセス許可。Amazon Chime Voice Connector では、メディアインサイトパイプライン設定を取得するために、これらのアクセス許可が必要です。詳細については、「通話分析を使用するように Voice Connector を設定する」を参照してください。	2023 年 4 月 14 日

Voice Connector のタグ付け	管理者は Amazon Chime SDK Voice Connector にタグを割り当てることができるようになりました。タグは、定義したキーと値のペアの形式でメタデータを割り当てます。詳細については、「Voice Connector でのタグの使用」を参照してください。	2023 年 4 月 13 日
新規および更新されたサービスにリンクされたロールポリシー	デベロッパーは AmazonChimeSDKEvents サービスにリンクされたロールを使用して、Kinesis Firehose などのストリーミングサービスにアクセスできます。詳細については、「 AmazonChimeSDKEvents サービスにリンクされたロールの使用」を参照してください。また、「サービスにリンクされたロールの使用」にAmazonChimeVoiceConnectorServiceLinkedRoleポリシー名を追加しました。詳細については、「 AmazonChimeVoiceConnectorServiceLinkedRoleポリシーの使用」を参照してください。	2023 年 3 月 27 日

通話分析と音声分析	管理者および管理者権限を持つデベロッパーは、通話分析で使用する Voice Connector を設定できます。必要に応じて、音声分析を有効にすることもできます。詳細については、このガイドの「Amazon Chime SDK 通話分析の管理」および「通話分析を使用するための Voice Connector の設定」を参照してください。	2023 年 3 月 27 日
更新されたセキュリティポリシー	AWS マネージド Amazon Chime SDK ポリシーに、Amazon Chime SDK Media Pipeline APIs を使用して Media Pipelines を作成、読み取り、削除できる新しいアクセス許可が追加されました。	2023 年 1 月 10 日
SIP シグナリングの新しいAWSリージョン	管理者は、SIP メディアアプリケーションをアジア、カナダ、欧州のAWSリージョンに関連付けることができるようになりました。詳細については、「ネットワーク設定と帯域幅要件」を参照してください。	2022 年 11 月 18 日
Alexa のスキル向上呼び出し	Alexa スキルデベロッパーは、スキルから直接 を呼び出すことができるようになりました。詳細については、「Amazon Chime SDK Alexa スキル呼び出しの有効化」を参照してください。	2022 年 11 月 18 日

緊急通報 911 を更新	緊急通報プロセスを更新しました。詳細については、「緊急通報の設定」を参照してください。	2022 年 8 月 4 日
新しいサービスにリンクされたロール	新しいサービスにリンクされたロールにより、デベロッパーは Amazon Chime SDK 会議でメディアパイプラインを使用できます。詳細については、「AWS マネージドポリシー：AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy」を参照してください。	2022 年 4 月 26 日
「Amazon Chime SDK 管理ガイド」の公開	Amazon Chime SDK 管理ガイドが公開されました。2022 年 3 月以前の変更については、「Amazon Chime 管理者ガイド」の「Amazon Chime のドキュメント履歴」を参照してください。	2022 年 3 月 24 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。

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。