



管理ガイド

# Amazon Chime SDK



# Amazon Chime SDK: 管理ガイド

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標とトレードドレスは、Amazon 以外の製品またはサービスとの関連において、顧客に混乱を招いたり、Amazon の名誉または信用を毀損するような方法で使用することはできません。Amazon が所有していない他のすべての商標は、それぞれの所有者の所有物であり、Amazon と提携、接続、または後援されている場合とされていない場合があります。

# Table of Contents

Amazon Chime SDK とは .....	1
料金 .....	1
前提条件 .....	2
Amazon Web Services アカウントの作成 .....	2
にサインアップする AWS アカウント .....	2
管理アクセスを持つユーザーを作成する .....	3
セキュリティ .....	5
ID およびアクセス管理 .....	6
対象者 .....	6
アイデンティティを使用した認証 .....	7
ポリシーを使用したアクセスの管理 .....	10
Amazon Chime SDK と IAM の連携方法 .....	13
Amazon Chime SDK アイデンティティベースのポリシー .....	13
リソース .....	14
例 .....	14
音声分析での暗号化の使用 .....	14
保管時の暗号化について .....	15
音声分析でグラントがどのように使用されるかを理解する .....	15
音声分析のキーポリシー .....	16
暗号化コンテキストの使用 .....	17
暗号化キーのモニタリング .....	18
サービス間の混乱した代理の防止 .....	24
Amazon Chime SDK リソースベースのポリシー .....	25
Amazon Chime SDK タグに基づく認可 .....	25
Amazon Chime SDK IAM ロール .....	25
Amazon Chime SDK での一時的な認証情報の使用 .....	25
サービスリンクロール .....	26
サービスロール .....	26
アイデンティティベースポリシーの例 .....	26
ポリシーのベストプラクティス .....	27
AWS マネージド Amazon Chime SDK ポリシー .....	27
AWS マネージドポリシー: AmazonChimeVoiceConnectorServiceLinkedRolePolicy .....	29
AWS 管理ポリシー: AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy .....	30
ポリシーの更新 .....	32

トラブルシューティング .....	36
Amazon Chime SDK でアクションを実行する権限がない .....	36
iam:PassRole を実行する権限がない .....	37
サービスリンクロールの使用 .....	37
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 .....	38
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 .....	42
メディアパイプラインでのロールの使用 .....	45
AmazonChimeSDKEvents サービスにリンクされたロールの使用 .....	48
ロギングとモニタリング .....	49
によるモニタリング CloudWatch .....	50
による自動化 EventBridge .....	63
AWS CloudTrail を使用して API コールをログに記録する .....	68
コンプライアンス検証 .....	71
耐障害性 .....	72
インフラストラクチャセキュリティ .....	73
開始 .....	74
Amazon Chime SDK アカウントの電話番号の設定 .....	74
電話番号の管理 .....	75
電話番号のプロビジョニング .....	76
国際電話番号のリクエスト .....	79
必要書類の提出 .....	80
発信通話の制限 .....	81
国別電話番号要件 .....	82
既存の電話番号の移植 .....	98
番号を移植するための前提条件 .....	99
電話番号を Amazon Chime SDK に移植する .....	99
必要書類の提出 .....	80
リクエストステータスの表示 .....	102
ポート番号の割り当て .....	102
Amazon Chime SDK から電話番号を移植する方法 .....	103
電話番号の移植ステータスの定義 .....	106
電話番号インベントリの管理 .....	107
ボイスコネクタへの電話番号の割り当て .....	107
音声コネクタ番号の再割り当て .....	109
Voice Connectorの電話番号の割り当て解除 .....	110
電話番号の再割り当て .....	110

SIP メディアアプリケーションへの電話番号の割り当て .....	111
電話番号の詳細を表示する .....	111
電話番号の製品タイプを変更する .....	111
電話番号の割り当てタイプを変更します。 .....	112
アウトバウンドコール名を設定する .....	113
電話番号を削除する .....	114
削除された電話番号の復元 .....	115
発信通話の評価を最適化する .....	115
ステップ 1: 希望する連絡方法を把握する .....	116
ステップ 2: 通話をブランド化する .....	116
ステップ 3: わかりやすい発信者 IDs .....	116
ステップ 4: 有効な電話番号を呼び出す .....	117
ステップ 5: 最適なタイミングで を呼び出す .....	117
ステップ 6: 通話 ID の評価を監視する .....	117
ステップ 7: 複数の数値を使用する .....	117
ステップ 8: アプリベンダーと連携する .....	118
ステップ 9: アウトリーチ戦略にメッセージを追加して、あなたが誰であることを顧客に知らせる .....	118
ステップ 10: 戦略を検証する .....	118
Voice Connector の管理 .....	119
開始する前に .....	120
Voice Connector の作成 .....	121
Voice Connector でのタグの使用 .....	122
Voice Connector へのタグの追加 .....	122
タグの編集 .....	122
タグの削除 .....	123
Voice Connector 設定の編集 .....	123
電話番号の割り当ておよび割り当て解除 .....	130
Voice Connector の削除 .....	131
通話分析を使用するように Voice Connector を設定する .....	131
Voice Connector グループの管理 .....	132
Amazon Chime SDK Voice Connector グループの作成 .....	133
Amazon Chime SDK Voice Connector グループの編集 .....	133
Voice Connector グループへの電話番号の割り当てと割り当て解除 .....	134
Amazon Chime SDK Voice Connector グループの削除 .....	135
Kinesis へのメディアのストリーミング .....	136

メディアストリーミングの開始 .....	137
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 .....	138
Voice Connector での Amazon Chime SDK 音声分析の使用 .....	139
Voice Connector 設定ガイドの使用 .....	140
通話分析の管理 .....	141
通話分析を設定する .....	141
前提条件 .....	142
通話分析設定の作成 .....	142
通話分析の設定を使用する .....	149
通話分析設定の更新 .....	149
通話分析設定の削除 .....	149
音声分析の有効化 .....	150
音声プロファイルドメインの管理 .....	152
音声プロファイルドメインの作成 .....	153
音声プロファイルドメインの編集 .....	153
音声プロファイルドメインの削除 .....	154
音声プロファイルドメインでのタグの使用 .....	154
音声分析の同意通知について .....	156
緊急通報の設定 .....	158
緊急通報の住所の検証 .....	158
サードパーティー緊急ルーティング番号の設定 .....	159
緊急通報での PIDF-LO の使用 .....	160
SIP メディアアプリケーションの管理 .....	163
SIP アプリケーションとルールについて .....	164
SIP メディアアプリケーションの使用 .....	165
SIP メディアアプリケーションの作成 .....	165
SIP メディアアプリケーションでのタグの使用 .....	166
SIP メディアアプリケーションの表示 .....	168
SIP メディアアプリケーションの更新 .....	168
SIP メディアアプリケーションの削除 .....	169
SIP ルールの管理 .....	171
SIP ルールの作成 .....	171
SIP ルールの表示 .....	173
SIP ルールの更新 .....	173
SIP ルールの有効化 .....	174
SIP ルールの無効化 .....	175

---

SIP ルールの削除 .....	176
グローバル設定の管理 .....	177
通話詳細レコードの設定 .....	177
Amazon Chime SDK Voice Connector 通話詳細レコード .....	178
Amazon Chime SDK Voice Connector ストリーミング詳細レコード .....	179
ネットワーク設定と帯域幅の要件 .....	180
共通 .....	180
Amazon Chime SDK WebRTC メディアセッション .....	180
Amazon Chime SDK Voice Connector .....	181
SIP シグナリング .....	181
メディア .....	182
キャリア、メディアデステイネーション、ポート向けの Amazon ボイスフォーカス .....	183
帯域幅の要件 .....	183
管理サポート .....	185
ドキュメント履歴 .....	186
.....	cxc

# 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](#)にアクセスして Amazon Chime 管理者 AWS 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

- [にサインアップする AWS アカウント](#)
- [管理アクセスを持つユーザーを作成する](#)

### にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

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、電話キーパッドで検証コードを入力するように求められます。

にサインアップすると AWS アカウント、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、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用して[ルートユーザーアクセスが必要なタスク](#)を実行してください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。<https://aws.amazon.com/> の [マイアカウント] を選んで、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理できます。

## 管理アクセスを持つユーザーを作成する

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

### のセキュリティ保護 AWS アカウントのルートユーザー

1. ルートユーザーを選択し、AWS アカウント E メールアドレスを入力して、アカウント所有者 [AWS Management Console](#) として 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 ユーザーガイドの「[ルートユーザーとしてサインインする](#)」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「[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。

### 管理アクセスを持つ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、ユーザーに管理アクセスを付与します。

を ID ソース IAM アイデンティティセンターディレクトリとして使用する方法のチュートリアルについては、「[ユーザーガイド](#)」の「[デフォルトでユーザーアクセス IAM アイデンティティセンターディレクトリを設定する AWS IAM Identity Center](#)」を参照してください。

### 管理アクセス権を持つ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 Identity Center ユーザーを使用してサインインする方法については、「AWS サインインユーザーガイド」の [AWS 「アクセスポータルにサインインする」](#) を参照してください。

## 追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

手順については、「AWS IAM Identity Center ユーザーガイド」の「[権限設定を作成する](#)」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

手順については、「AWS IAM Identity Center ユーザーガイド」の「[グループの参加](#)」を参照してください。

# Amazon Chime SDK のセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、AWS とユーザーの間で共有される責任です。[責任共有モデル](#)では、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ — 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 AWS は AWS にあります。AWS は、安全に使用できるサービスも提供します。コンプライアンス [AWS プログラム](#) コンプライアンスプログラムの一環として、サードパーティーの監査者は定期的にセキュリティの有効性をテストおよび検証。Amazon Chime SDK に適用されるコンプライアンスプログラムの詳細については、「[コンプライアンスプログラムによる 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。
- クラウドのセキュリティ — お客様の責任は、使用する AWS サービスによって決まります。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 を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するように Amazon Chime SDK を設定する方法について説明します。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 Identity and Access Management](#)
- [Amazon Chime SDK と IAM の連携方法](#)
- [音声分析での暗号化の使用](#)
- [サービス間の混乱した代理の防止](#)
- [Amazon Chime SDK リソースベースのポリシー](#)
- [Amazon Chime SDK タグに基づく認可](#)
- [Amazon Chime SDK IAM ロール](#)
- [Amazon Chime SDK アイデンティティベースのポリシーの例](#)
- [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](#)

- [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 AWS のサービス するのに役立つです。IAM 管理者は、誰を認証 (サインイン) し、誰に 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、追加料金なしで AWS のサービス 使用できる です。

### トピック

- [対象者](#)
- [アイデンティティを使用した認証](#)
- [ポリシーを使用したアクセスの管理](#)

## 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 – Amazon Chime SDK サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が与えられます。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、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。お客様の会社で Amazon Chime SDK で IAM 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 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](#)。

## アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証 ( にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーテッド ID AWS として にサインインできます。AWS IAM Identity Center ( 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 の認証情報は、フェデレーテッド ID の例です。フェデレーテッド ID 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 AWS を使用して にアクセスすると、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。へのサインインの詳細については AWS、「ユーザーガイド」の「[にサインインする方法 AWS アカウント](#)AWS サインイン」を参照してください。

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用して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。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、IAM [ユーザーガイドの API AWS 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、追加セキュリティ情報の提供をリクエストさ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を強化するために多要素認証 (MFA) を使用することをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「[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

を作成するときは AWS アカウント、アカウント内のすべての AWS のサービス およびリソースへの完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント 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でアクセスできます。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、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウントを持つ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許可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、特定のアクセス許可 AWS アカウントを持つ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 AWS Management Console ことで、[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、または AWS API AWS CLI 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。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーテッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーテッド ID が認証されると、その ID は



ロールに関連付けられ、ロールで定義されている許可が付与されます。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「[Creating a role for a third-party Identity Provider](#)」(サードパーティーアイデンティティプロバイダー向けロールの作成)を参照してください。IAM Identity Center を使用する場合は、許可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。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「[アクセス許可セット](#)」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、(ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスの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 でのクロスアカウントリソースアクセス](#)」を参照してください。
- クロスサービスアクセス — 一部の は、他の の機能 AWS のサービス を使用します AWS のサービス。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許可、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 でアクションを実行する場合 AWS、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、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。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 のサービスにアクセス許可を委任するロールの作成](#)」を参照してください。
- サービスにリンクされたロール - サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行する



ロールを引き受けることができます。サービスにリンクされたロールは、AWS アカウント、サービスによって所有されます。IAM 管理者は、サービスリンクロールの許可を表示できますが、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 – IAM ロールを使用して、EC2 インスタンスで実行され、AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。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、インスタンスにアタッチ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の管理

でアクセスを制御する AWS には、ポリシーを作成し、AWS ID またはリソースにアタッチします。ポリシーは AWS、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義するオブジェクトです。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きに、これらのポリシー AWS 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。ほとんどのポリシーは JSON ドキュメント AWS として保存されます。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 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。

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、アクションの許可を定義します。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。そのポリシーを持つユーザーは、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のポリシー

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、および条件をコントロールします。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のポリシーは、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ています。管理ポリシーは、内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。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、フェデレーテッドユーザー、またはを含めることができます AWS のサービス。

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

## 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、自分でポリシーを記述するよりも、AWS 管理ポリシーを使用する方が簡単です。チームに必要な許可のみを提供する [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。すぐに開始するには、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としており、AWS アカウントで利用できます。AWS 管理ポリシーの詳細については、「IAM ユーザーガイド」の「[AWS 管理ポリシー](#)」を参照してください。

AWS サービスは、AWS 管理ポリシーを維持および更新します。AWS 管理ポリシーのアクセス許可は変更できません。サービスは、AWS マネージドポリシーに新しい機能をサポートするために追加のアクセス許可を追加することがあります。この種の更新は、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、ロール) に影響を与えます。サービスは、新機能の起動時または新しいオペレーションが利用可能になったときに、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アクセス許可を削除しないため、ポリシーの更新によって既存のアクセス許可が中断されることはありません。

さらに、は、複数の サービスにまたがる職務機能の マネージドポリシー AWS をサポートします。例えば、ReadOnlyAccess AWS 管理ポリシーは、すべての AWS サービスとリソースへの読み取り専用アクセスを提供します。サービスが新機能を起動すると、は新しいオペレーションとリソースの読み取り専用アクセス許可 AWS 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許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、AWS WAF、および Amazon VPC は、ACLs。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 は、一般的ではない追加のポリシータイプをサポートします。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。

- **アクセス許可の境界** - アクセス許可の境界は、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) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可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アクセス許可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、アクセス許可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。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「[IAM エンティティのアクセス許可の境界](#)」を参照してください。
- **サービスコントロールポリシー (SCPs)** – SCPs は、 の組織または組織単位 (OU) に対する最大アクセス許可を指定する JSON ポリシーです AWS Organizations。AWS Organizations は、AWS

アカウント ビジネスが所有する複数の をグループ化して一元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、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。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があります。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](#)」を参照してください。

## 複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される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与する場合にリクエストを許可するかどうか AWS を決定する方法については、IAM ユーザーガイドの「[ポリシー評価ロジック](#)」を参照してください。

## 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 機能について学習します。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、関連付けられた 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許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数の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 は、ポリシーでのリソース ARNs 指定をサポートしています。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
- キー暗号化マテリアルのローテーション
- 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。AWS Key Management Service

## 保管時の暗号化について

デフォルトでは、音声分析は保管中のすべてのユーザーデータを暗号化します。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の暗号化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、スピーカーを音声埋め込みに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。権限の詳細については、次のセクションを参照してください。

## 音声分析でグラントがどのように使用されるかを理解する

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、AWS KMS に `CreateGrant` リクエストを送信して、ユーザーに代わってグラントを作成します。次の内部オペレーションでキーを使用するには、グラントが必要です。

- 指定された対称カスタマーマネージドキー ID [DescribeKey](#) が有効であることを確認するリクエストを AWS KMS に送信します。
- オブジェクトを暗号化するデータキーを作成するための KMS キーへの [GenerateDataKey](#) リクエストの送信。
- AWS KMS に [Decrypt](#) リクエストを送信して、暗号化されたデータキーを復号して、データの暗号化に使用できるようにします。
- AWS KMS 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。

グラントへのアクセスを取り消すことも、サービスのキーへのアクセスを削除することもできます。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、話者検索ワークフローで `AccessDeniedException` エ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、「[Key Management Service デベロッパーガイド](#)」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。AWS

キーアクセスのトラブルシューティングについては、「[Key AWS 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。AWS KMS 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、AWS KMS 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。キーは `aws:chime:voice-profile-domain:arn` 値はリソース 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、権限に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、権限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 AWS KMS にリクエストを送信します。こ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": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE: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 は一意のデータキーを作成して、各スピーカーの登録音声を暗号化します。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/00000000-1111-2222-3333-999999999999"
  }],
  "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": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE: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。

では AWS、サービス間のなりすましは、混乱した代理シナリオにつながる可能性があります。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、アカウントのリソースへのマネージドアクセス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。



## サービスリンクロール

[サービスにリンクされたロール](#)を使用すると、AWS サービスがユーザーに代わってアクションを実行する他のサービスのリソースにアクセスできます。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 ユーザーとロールには 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。また、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はできません。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](#)
- [AWS マネージド Amazon Chime SDK ポリシー](#)

- [AWS マネージドポリシー: AmazonChimeVoiceConnectorServiceLinkedRolePolicy](#)
- [AWS 管理ポリシー: AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy](#)
- [AWS マネージドポリシーに対する Amazon Chime の更新](#)

## 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 管理ポリシーの使用を開始する - Amazon Chime SDK の使用をすばやく開始するには、AWS 管理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によるアクセス許可の使用を開始する](#)」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 マネージドを使用して AmazonChimeVoiceConnectorServiceLinkedRolePolicy、ユーザーに Amazon Chime SDK アクションへのアクセスを許可します。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:

### AmazonChimeVoiceConnectorServiceLinkedRolePolicy

AmazonChimeVoiceConnectorServiceLinkedRolePolicy により、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 を使用して音声を作成できます。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) および Amazon Simple Queue Service (SQS) への通知イベントの送信、Amazon Polly を使用した音声合成のアクセス許可を付与します。

```
{  
  "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 管理ポリシー:

### 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、メトリクスを に発行できます 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 会議にアクセスできるようになります。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。

#### アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `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、メディアへの配置、データ保持間隔の更新、データストリームの説明、データストリームの作成、データストリームのリストを行うための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 の更新

次の表は、Amazon Chime SDK IAM ポリシーに加えられた更新の一覧と説明です。

変更	説明	日付
<a href="#">AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy</a> – 既存ポリシーの更新	Amazon Chime SDK ミーティングが にメトリクスを発行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、「 <a href="#">Amazon Chime SDK メディアパイプラインでのロールの使用</a> 」を参照してください。	2023 年 12 月 8 日
<a href="#">AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy</a> – 既存ポリシーの更新	Kinesis Video Streams が Amazon Chime SDK 会議にオーディオ、ビデオ、画面	2023 年 8 月 20 日

変更	説明	日付
	<p>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、「<a href="#">Amazon Chime SDKメディアパイプラインでのロールの使用</a>」を参照してください。</p>	
<p><a href="#">AmazonChimeVoiceConnectorServiceLinkedRolePolicy</a> – 既存ポリシーへの更新</p>	<p><a href="#">GetMediaInsightsPipelineConfiguration</a> API へのアクセスを許可するAmazonChimeVoiceConnectorServiceLinkedRolePolicy 追加されたアクセス許可。Amazon Chime Voice Connector では、メディアインサイトパイプラインの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、「<a href="#">通話分析を使用するように Voice Connectorを設定する</a>」を参照してください。</p>	<p>2023 年 4 月 14 日</p>



変更	説明	日付
新規および更新されたサービスにリンクされたロール	開発者は 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、 <a href="#">AmazonChimeSDKEvents「サービスにリンクされたロールの使用」</a> を参照してください。また、「 <a href="#">サービスにリンクされたロールの使用</a> 」に <a href="#">AmazonChimeVoiceConnectorServiceLinkedRolePolicy</a> 名前を追加しました。詳細については、「 <a href="#">の使用 AmazonChimeVoiceConnectorServiceLinkedRolePolicy</a> 」を参照してください。	2023 年 3 月 27 日
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。	<a href="#">AWS マネージド Amazon Chime SDK ポリシー</a> に、 <a href="#">Amazon Chime SDK メディアパイプライン APIs</a> 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
<a href="#">AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy</a> - 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 ミーティング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にリンクされたロールが追加されました。	2022 年 4 月 27 日

変更	説明	日付
<p><a href="#">AWS 管理ポリシー: AmazonChimeVoiceConnectorServiceLinkedRolePolicy</a> – 既存のポリシーへの更新。</p>	<p>Amazon Chime SDK Voice Connector に、Amazon Polly を使用して音声を作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。</p>	<p>2022 年 3 月 15 日</p>
<p><a href="#">AmazonChimeVoiceConnectorServiceLinkedRolePolicy</a> – 既存ポリシーへの更新</p>	<p>Amazon Chime SDK Voice Connector に、Amazon Kinesis Video Streams へのアクセスを許可し、Amazon Simple Notification Service (Amazon SNS) と Amazon Simple Query Service (Amazon SQS) に通知イベントを送信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。</p>	<p>2021 年 12 月 20 日</p>

変更	説明	日付
既存のポリシーに関する変更。 <a href="#">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</a> 。	Amazon Chime SDK は、拡張検証をサポートする新しいアクションを追加しました。  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しました	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 の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちます。

### トピック

- [Amazon Chime SDK でアクションを実行する権限がない](#)
- [iam:PassRole を実行する権限がない](#)

### 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。

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

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:  
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 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

## iam:PassRole を実行する権限がない

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、管理者にお問い合わせ、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にリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

次の例のエラーは、という 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と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ために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がないため、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、以下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 [Speak](#) および [SpeakAndGetDigits](#) アクションを使用して音声を作成します。

## 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 サービスにリンクされたロールでサポートされているリージョン](#)

## 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 Connectors 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、次のサービスを信頼してロールを引き受けます。

- `voiceconnector.chime.amazonaws.com`

[AmazonChimeVoiceConnectorServiceLinkedRolePolicy](#) 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、または AWS API で Amazon Chime SDK SIP AWS Management Console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、サービス名を使用して `voiceconnector.chime.amazonaws.com` 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。このサービスリンクロールを削除しても、同じ方法でロールを再作成できます。

## 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した後は、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、モニタリングや保守が積極的に行わ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

リソースを削除しようとしたときに Amazon Chime SDK サービスがロールを使用している場合、削除が失敗する可能性があります。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。

によって使用されている 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 に送信する で、停止 を選択します。
  - f. [保存] を選択します。

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

- AWS CLI の `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) が使用する 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。

サービスリンクロールの手動による削除

IAM コンソール、または AWS API オペレーションを使用して AWS CLI、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 サービスにリンクされたロールでサポートされているリージョン

Amazon Chime SDK は、サービス AWS リージョンが利用可能な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](#)」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 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](#)
- [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 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](#)
- [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 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`。Amazon Chime SDK メディアパイプラインがユーザーに代わって AWS のサービスにアクセスできるようにします。

`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次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`、このガイドの前半の [AWS 管理ポリシー: 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`。

で AWS CLI、次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。このサービスリンクロールを削除しても、同じ方法でロールを再作成できます。

## 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した後は、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、または AWS API を使用して AWS

CLI、`AWSServiceRoleForAmazonChimeSDKMediaPipelines` 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 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、サービスが利用可能なすべての 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ています。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` を完了できません `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なくなった場合は、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、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、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 で実行す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 ユーザーガイド CloudWatch](#)」を参照してください。
- Amazon EventBridge は、AWS resources の変更を記述する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、特定のイベントを監視するルールを作成し、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 を使用すると、Amazon EC2 インスタンスやその他のソースからログファイルをモニタリング、保存 CloudTrail、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、またはアカウントに代わって行われた API コールおよび関連イベントをキャプチャします。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。を呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、呼び出しが発生した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 による Amazon Chime SDK のモニタリング CloudWatch](#)
- [による Amazon Chime SDK の自動化 EventBridge](#)
- [AWS CloudTrail を使用して API コールをログに記録する](#)

## Amazon による 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。CloudWatch は raw データを収集し、読み取り可能なほぼリアルタイムの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の確に把握できます。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、次のメトリクスを に送信します。Amazon Chime SDK CloudWatch は、通話中にメトリクスを 1 分に 1 回送信し、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、通話中に累積されます。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の分だけ引き継がれます。呼び出しの終了時に、単一のパケット損失メトリクスを受け取りません。

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。 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

メトリクス	説明
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
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

メトリクス	説明
CustomerToVcRtpPackets	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 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
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、通話が終了するまで 1 分ごとに送信されます。値の数は累積的です。  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るパケットの平均ジッター。  単位: マイクロ秒

メトリクス	説明
VcToCustomerRtpPackets	<p>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 RTP パケットの数。</p> <p>単位: カウント</p>
VcToCustomerRtpBytes	<p>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。</p> <p>単位: カウント</p>
VcToCustomerRtcpPackets	<p>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 RTCP パケットの数。</p> <p>単位: カウント</p>
VcToCustomerRtcpBytes	<p>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。</p> <p>単位: カウント</p>
VcToCustomerPacketsLost	<p>Amazon Chime SDK Voice Connector インフラストラクチャから顧客への転送中に失われたパケットの数。値は、通話が終了するまで 1 分ごとに送信されます。値の数は累積的です。</p> <p>単位: カウント</p>
VcToCustomerJitter	<p>Amazon Chime SDK Voice Connector インフラストラクチャから顧客に送信されるパケットの平均ジッター。</p> <p>単位: マイクロ秒</p>

メトリクス	説明
RTTBetweenVcAndCustomer	<p>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。</p> <p>単位: マイクロ秒</p>
MOSBetweenVcAndCustomer	<p>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ポインションスコア (MOS)。</p> <p>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。</p>
RemoteToVcRtpPackets	<p>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。</p> <p>単位: カウント</p>
RemoteToVcRtpBytes	<p>リモートエンドから RTP パケット内の 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。</p> <p>単位: カウント</p>
RemoteToVcRtcpPackets	<p>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。</p> <p>単位: カウント</p>
RemoteToVcRtcpBytes	<p>リモートエンドから RTCP パケット内の 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。</p> <p>単位: カウント</p>

メトリクス	説明
RemoteToVcPacketsLost	<p>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、通話が終了するまで 1 分ごとに送信されます。値の数は累積的です。</p> <p>単位: カウント</p>
RemoteToVcJitter	<p>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るパケットの平均ジッター。</p> <p>単位: マイクロ秒</p>
VcToRemoteRtpPackets	<p>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。</p> <p>単位: カウント</p>
VcToRemoteRtpBytes	<p>Amazon Chime SDK Voice Connector インフラストラクチャから RTP パケットのリモートエンドに送信されたバイト数。</p> <p>単位: カウント</p>
VcToRemoteRtcpPackets	<p>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。</p> <p>単位: カウント</p>
VcToRemoteRtcpBytes	<p>Amazon Chime SDK Voice Connector インフラストラクチャから RTCP パケットのリモートエンドに送信されたバイト数。</p> <p>単位: カウント</p>

メトリクス	説明
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、通話が終了するまで 1 分ごとに送信されます。値の数は累積的です。  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る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
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する推定平均オリジンスコア (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 デイメンション

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

デイメンション	説明
VoiceConnectorId	メトリクスを表示する Amazon Chime SDK Voice Connector の識別子。



ディメンション	説明
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

Amazon Chime SDK Voice Connector を設定して、メトリクスを CloudWatch ログに送信できます。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、詳細なメトリクスを 1 分に 1 回送信します。Amazon Chime SDK は、設定された Voice Connector で行われたすべての呼び出しに対してそれらを送信し、ユーザーに代わって作成した Logs CloudWatch ロググループに送信します。

ロググループ名は、次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、通話中に累積されます。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の分だけ引き継がれます。呼び出しの終了時に、単一のパケット損失メトリクスを受け取ります。

Amazon Chime SDK には、JSON 形式のログに次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。

フィールド	説明
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。Logs Insights CloudWatch を使用します。詳細については、 <a href="#">「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」</a> を参照してください。 CloudWatch
aws_region	呼び出しの AWS リージョン。
cust2vc_rtp_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 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。

フィールド	説明
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、通話が終了するまで 1 分ごとに送信されます。値の数は累積的です。
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る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顧客に送信された 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顧客に送信された RTCP パケットの数。
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顧客への転送中に失われたパケットの数。値は、通話が終了するまで 1 分ごとに送信されます。値の数は累積的です。
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る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。

フィールド	説明
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ポインションスコア (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 パケット内の 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 パケット内の 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_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、通話が終了するまで 1 分ごとに送信されます。値のカウントは累積です。
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る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。

フィールド	説明
vc2rem_rtp_bytes	Amazon Chime SDK Voice Connector インフラストラクチャから RTP パケットの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 パケットの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、通話が終了するまで 1 分ごとに送信されます。値のカウントは累積です。
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るパケットの平均ジッター。
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する推定平均オリジンスコア (MOS)。

## SIP メッセージログ

Amazon Chime SDK Voice Connector の SIP メッセージログの受信を選択できます。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、自動的に作成された Logs CloudWatch 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 コール ID。
sip_message	キャプチャされた完全な SIP メッセージ。

## による 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、ベストエフォート配信 EventBridge のために送信されます。つまり、Amazon Chime SDK はすべてのイベントを送信しようとしませんが 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「[のサービスからの AWS 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。Key AWS 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 に対して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 ユーザーガイド EventBridge」](#)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 イベントを送信することをサポートします。

#### 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 ストリーミングの終了

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"
  }
}
```

## AWS CloudTrail を使用して API コールをログに記録する

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など、Amazon Chime SDK のすべての API 呼び出しをイベントとして 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、CloudTrail コンソールのイベント履歴ページ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、CloudTrail はそのアクティビティをイベントに記録します。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、[「イベント履歴を含む 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。

以下のトピックをリストされた順序で実行します。

1. [「証跡作成の概要」](#)
2. [CloudTrail がサポートするサービスと統合](#)
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 `CreateAttendee`、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。同一性情報は次の判断に役立ちます。

- 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 サービスによって行われたかどうか。

詳細については、[CloudTrailuserIdentity 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。イベントは任意ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどの情報を含みます。CloudTrail ログファイルはパブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

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": "00fbee1-123e-111e-93e3-11111bfbfcc1",
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012"
}
```

## Amazon Chime SDK のコンプライアンス検証

サードパーティーの監査者は、SOC、PCI、FedRAMP、HIPAA などの複数の AWS コンプライアンスプログラムの一環として、AWS 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 [AWS のサービスによる対象範囲内のコンプライアンスプログラム](#) を参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、[AWS「コンプライアンスプログラム」](#) を参照してください。

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

を使用する際のお客様のコンプライアンス責任 AWS のサービスは、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。では、コンプライアンスに役立つ以下のリソース AWS 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 AWS を にデプロイする手順について説明します。
- [アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャー](#) – このホワイトペーパーでは、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について説明します。

**Note**

すべて AWS のサービス HIPAA の対象とな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 コンプライアンスリソース](#) – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- [AWS カスタマーコンプライアンスガイド](#) – コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- 「[デベロッパーガイド](#)」の「[ルールによるリソースの評価](#)」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。AWS Config
- [AWS Security Hub](#) – これにより AWS のサービス、内のセキュリティ状態を包括的に確認できます AWS。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。
- [Amazon GuardDuty](#) – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービスを検出します。GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件への対応に役立ちます。
- [AWS Audit Manager](#) – これにより AWS のサービス、AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

## Amazon Chime SDK の耐障害性

AWS グローバルインフラストラクチャは、AWS リージョンとアベイラビリティゾーンを中心に構築されています。AWS リージョンは、低レイテンシー、高スループット、および高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティゾーンを提供します。アベイラビリティゾーンでは、ゾーン間で中断することなく自動的にフェ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。アベイラビリティゾーン

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が高く、フォールトトレラントで、スケーラブルです。

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

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をサポートするのに役立つ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

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

が AWS 公開している API コールを使用して、ネットワーク経由で にアクセスします。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 は必須で TLS 1.3 がお勧めです。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

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



# 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 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](#)
- [国際電話番号のリクエスト](#)
- [既存の電話番号の移植](#)
- [電話番号インベントリの管理](#)
- [電話番号を削除する](#)
- [削除された電話番号の復元](#)
- [発信通話の評価を最適化する](#)

## 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、「都道府県」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。

国際番号を購入するには、多くの国の規制により次の品目の所持が義務付けられています。

- 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. <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. まだ選択されていない場合は、[アカウントと請求] を選択します。
4. [サービス] には [Chime SDK (番号管理)] を選択します。
5. [カテゴリ] で [電話番号リクエスト] を選択し、[次のステップ:追加情報] を選択します。
6. [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。
7. [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
8. [E 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 は、電話番号を登録できるかどうかを知らせる電子メールでサポートリクエストに回答します。番号がプロビジョニングされると、Amazon Chime SDK コンソールでそれらを表示できます。[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。

9. 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。

## 必要書類の提出

要求された電話番号を受け取ったら、必要な書類をすべて提出します。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。

## 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をサポートしていますが、中国への通話を承認されたすべてのお客は、次の条件を満たしている必要があります。

#### 資格基準

##### サポートされていないユースケース

- 短時間の呼び出しと 15 秒未満のアラート。
- 大量の通話、特に短期間、同じアウトバウンド発信者 ID (1 分あたり 5 回以上) を使用します。
- 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 および/または TO 番号を使用した繰り返しの呼び出し。
- 事前承認されていない任意の番号から中国を呼び出そうとします。

##### サポートされているユースケース

- ホテルや IT サポート機能などの既知の事業体への直接電話。
- 大学の配置スキームや製品購入など、ビジネスへの関与を試みるユーザーを呼び出します。

#### 設定に必要なデータ

中国の電話番号 (+86) を呼び出す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、会社名を識別する発表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知ることができます。
- 中国を呼び出すためのユースケースの詳細な説明を AWS に提供し、このトピックで説明されている適格性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結果

Amazon Chime SDK には、中国への呼び出しに対する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 アカウントは停止します。Amazon Chime SDK 管理者は、組織の他のメンバーにもこのポリシーを伝えて、これらの制限を認識してもらう必要があります。ルールの無視は、違反の許容可能な理由ではありません。

### 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、中国を呼び出す能力に影響を与える場合、[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	<ul style="list-style-type: none"> <li>• 勤務先住所</li> <li>• 所在地の証明</li> </ul> <p>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。</p>

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
	通話料無料	はい	<ul style="list-style-type: none"> <li>勤務先住所</li> </ul> <p>国際住所が許容されます。</p>

## 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	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> <li>認証書</li> </ul>
	通話料無料	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> <li>認証書</li> </ul>

## 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	<ul style="list-style-type: none"> <li>勤務先住所</li> <li>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</li> </ul>

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
			<p>通信接続サービスの証明。</p> <p>- または -</p> <p>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。</p> <p>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。</p>
	国内地域番号: +43720	はい	<ul style="list-style-type: none"> <li>勤務先住所</li> </ul> <p>住所は国内に存在する必要がある</p>
	通話料無料	はい	<ul style="list-style-type: none"> <li>勤務先住所</li> </ul> <p>許容外部アドレス</p>

## 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	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> </ul>

サポートされる製品タイプ	番号タイプ	必須 ID
		<ul style="list-style-type: none"> <li>• 認証書</li> </ul>
	通話料無料	<ul style="list-style-type: none"> <li>• 現在のプロバイダーからの最終請求書</li> <li>• 認証書</li> </ul>

## 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	<ul style="list-style-type: none"> <li>• 現在のプロバイダーからの最終請求書</li> <li>• 認証書</li> </ul>
	通話料無料	<ul style="list-style-type: none"> <li>• 現在のプロバイダーからの最終請求書</li> <li>• 認証書</li> </ul>

## 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	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> <li>認証書</li> </ul>
	通話料無料	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> <li>認証書</li> </ul>

## 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	<ul style="list-style-type: none"> <li>勤務先住所</li> <li>所在地の証明</li> </ul>

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
			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	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> <li>認証書</li> </ul>
	通話料無料	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> <li>認証書</li> </ul>

## 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	<ul style="list-style-type: none"> <li>勤務先住所</li> <li>事業者登録のコピー、または個人の場合は ID のコピー</li> <li>公共料金領収書などの住所証明</li> </ul> <p>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。</p>
	国内地域番号: +49 32	はい	<ul style="list-style-type: none"> <li>勤務先住所</li> <li>事業者登録のコピー、または個人の場合は ID のコピー</li> <li>公共料金領収書などの住所証明</li> </ul> <p>住所は国内に存在する必要がある</p>
	通話料無料	はい	<ul style="list-style-type: none"> <li>勤務先住所</li> <li>公共料金領収書などの住所証明</li> </ul> <p>住所は国内に存在する必要がある</p>



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
			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	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> <li>認証書</li> <li>勤務先住所</li> <li>事業者登録のコピー</li> <li>会社代表者 ID のコピー</li> </ul> <p>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。</p>
	通話料無料	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> <li>認証書</li> <li>NRA から入手した番号証明書</li> </ul> <p>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、</p>

サポートされる製品タイプ	番号タイプ	必須 ID
		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	<ul style="list-style-type: none"> <li>勤務先住所</li> </ul> <p>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。</p>
	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	<ul style="list-style-type: none"> <li>勤務先住所</li> </ul> <p>住所は国内に存在する必要がある</p>
	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	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> <li>認証書</li> </ul>

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	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> <li>認証書</li> </ul>

## 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	<ul style="list-style-type: none"> <li>勤務先住所</li> <li>所在地の証明</li> <li>事業者登録のコピー</li> <li>パスポートまたはエンドユーザーの ID</li> </ul> <p>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。</p>
	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	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> <li>認証書</li> <li>会社代表者のパスポートまたは ID のコピー</li> <li>現地の事業者登録のコピー、または個人の住所証明</li> </ul>
	通話料無料機能	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> <li>認証書</li> </ul>

## 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
	通話料無料	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> </ul>

サポートされる製品タイプ	番号タイプ	必須 ID
		<ul style="list-style-type: none"> <li>• 認証書</li> </ul>

## 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	<ul style="list-style-type: none"> <li>• 勤務先住所</li> </ul> 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	ローカル	いいえ	該当なし
Amazon Chime SDK Voice Connector			
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	<ul style="list-style-type: none"> <li>勤務先住所</li> <li>所在地の証明</li> </ul> <p>住所は国内に存在する必要がある</p>

## 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	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> <li>認証書</li> </ul>
	通話料無料	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> <li>認証書</li> </ul>

## 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	<ul style="list-style-type: none"> <li>勤務先住所</li> <li>所在地の証明</li> <li>事業者登録のコピー、または個人の場合は ID のコピー</li> </ul> <p>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。</p>
	外線発信番号: +41 051、+41 058	はい	<ul style="list-style-type: none"> <li>勤務先住所</li> </ul> <p>住所は国内に存在する必要がある</p>
	通話料無料	はい	<ul style="list-style-type: none"> <li>勤務先住所</li> <li>事業者登録のコピー、または個人の場合は ID のコピー</li> </ul> <p>許容外部アドレス</p>

### 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	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> <li>認証書</li> <li>勤務先住所</li> </ul> 許容外部アドレス
	通話料無料	<ul style="list-style-type: none"> <li>現在のプロバイダーからの最終請求書</li> <li>認証書</li> <li>勤務先住所</li> <li>NRA から入手した証明書</li> </ul> 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	<ul style="list-style-type: none"><li>現在のプロバイダーからの最終請求書</li><li>認証書</li></ul>
	通話料無料	<ul style="list-style-type: none"><li>現在のプロバイダーからの最終請求書</li><li>認証書</li></ul>

## 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せん。

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](#)
- [電話番号を Amazon Chime SDK に移植する](#)
- [必要書類の提出](#)
- [リクエストステータスの表示](#)
- [ポート番号の割り当て](#)
- [Amazon Chime SDK から電話番号を移植する方法](#)
- [電話番号の移植ステータスの定義](#)

## 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

- 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で生成されます。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

- Amazon Chime SDK 音声コネクタ番号を音声コネクタ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。

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。

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

Amazon Chime SDK から米国以外の電話番号を移植できます。番号の種類ごとに異なる手順に従います。必要に応じて以下のセクションを拡張して詳細をご覧ください。

### 米国番号の移植

Amazon Chime から番号を移植するには、受賞したキャリアに移植リクエストを送信します。受賞した通信事業者に情報を送信するときは、AWS 移管される電話番号に関連するアカウント ID としてアカウント ID を含めてください。

移管プロセスが終了し、当選した通信事業者がその番号を入手したら、その番号の割り当てを解除してインベントリから削除する必要があります。詳細については、このガイドの「[Voice Connector の電話番号の割り当て解除](#)」および「[電話番号を削除する](#)」を参照してください。

### Important

- 番号を移植できるかどうかは、受賞した運送業者がその番号を受け入れる能力によって異なります。

- 電話番号のセキュリティを確保するには、新しい通信事業者の移植リクエストの信頼性を検証することが重要です。アカウントの詳細が正しくない場合 (たとえば、アカウント ID が一致しない場合)、ポートアウトのリクエストが拒否され、遅延が発生し、リクエストの再送信が必要になることがあります。

### (オプション) 電話番号を保護するための PIN のリクエスト

セキュリティを強化するために、電話番号に PIN を適用するよう当社にご連絡ください。その後、当選した通信事業者はその PIN を使用します。以下の手順に従います。

PIN をリクエストするには

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、次のように入力します。

**I would like to assign a pin to my phone number: Pin: ABCD123 Phone Number: 1234567890**

**Note**

4 ~ 10 文字の英数字 PIN を入力する必要があります。

AWS Support は PIN を電話番号に関連付けます。受賞した通信事業者にポートを依頼するときは、AWS アカウント ID と PIN を入力してください。その情報を使用して、お客様の番号について受け取ったポートリクエストを検証します。

## 国際電話番号の移管

以下の手順では、Amazon Chime SDK から国際電話番号を移植する方法について説明します。

電話番号をポートアウトするには

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 適切な次のステップで応答します。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回答が届きます。

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、「[Voice Connectorの電話番号の割り当て解除](#)」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、「課題タイプ」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、それらの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。

- 「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」オプションまたは「音声コネクタグループ」オプションリストが表示されます。

- 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。
- [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せん。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、アウトバウンドコール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

- <https://console.aws.amazon.com/chime-sdk/home> にある Amazon Chime SDK コンソールを開きます。
- 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。
- 「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。
- [Details (詳細)] ページで、[Edit (編集)] を選択します。
- [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](#)
- [ステップ 2: 通話をブランド化する](#)
- [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](#)
- [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](#)
- [ステップ 5: 最適なタイミングで発信通話を行う](#)
- [ステップ 6: 発信者 ID の評価を監視する](#)
- [ステップ 7: 複数の番号を発信者 ID として使用する](#)

- [ステップ 8: アプリベンダーと連携する](#)
- [ステップ 9: アウトリーチ戦略にメッセージを追加して、あなたが誰であることを顧客に知らせる](#)
- [ステップ 10: 発信通話戦略を検証する](#)

## 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分からないことです。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、あなたが誰であることを顧客に知らせる

通話に応答しない場合は、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、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、発信通話と着信通話、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植したり、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の制限があります。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、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、そのグループに 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。

## 内容

- [開始する前に](#)
- [Amazon Chime SDK Voice Connector の作成](#)
- [Voice Connector でのタグの使用](#)
- [Amazon Chime SDK Voice Connector 設定の編集](#)
- [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 の削除](#)
- [通話分析を使用するように Voice Connector を設定する](#)
- [Amazon Chime SDK Voice Connector グループの管理](#)
- [Amazon Chime SDK Voice Connector メディアを Kinesis にストリーミングする](#)
- [Amazon Chime SDK Voice Connector 設定ガイドの使用](#)

## 開始する前に

Amazon Chime SDK Voice Connector を使用するには、IP Private Branch Exchange (PBX)、Session Border Controller (SBC)、または Session Initiation Protocol (SIP) をサポートするインターネットアクセスを備えた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。

から AWS オンプレミスの電話システムに送信される通話のセキュリティを確保するために、AWS と電話システムの間には SBC を設定することをお勧めします。Amazon Chime SDK Voice Connector シグナリングおよびメディア IP アドレスからの SBC への SIP トラフィックの一覧表示を許可しま



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 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. Voice Connector 名 に、Voice Connector 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、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 Secure RTP (SRTP) を使用するように Voice Connector が設定されます。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、の値CostCenterを持つ という名前のタグキーを作成し98765、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、誰が作成したかに関係なく、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、誰が作成したかに関係なく、AWS アカウント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. [変更を保存] を選択します。

## Amazon Chime SDK Voice Connector 設定の編集

Amazon Chime SDK Voice Connector を作成したら、発信通話と着信通話を許可する終了設定と発信設定を編集する必要があります。また、Kinesis へのストリーミングや緊急通話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、Voice Connector の設定を一連のタブにグループ化します。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。

## 一般設定の編集

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。

一般設定を変更するには

1. (オプション) 詳細 に、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. [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、ここで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を知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場合、SIP シグナリングには TLS、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、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 の説明に従って 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 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。インバウンドコールとアウトバウンドコールでは、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、これらの追加の 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につれて変化する可能性のある一連の IP アドレスに解決されるため、DNS 有効期限よりも長い時間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) 「許可されたホストリスト」で、「新規」を選択し、許可する CIDR 表記と値を入力し、「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ります。

-または-

CIDR 表記の編集と変更を選択します。

-または-

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、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。

## 送信元設定の編集

送信元設定は、Amazon Chime SDK Voice Connector へのインバウンド呼び出しに適用されます。インバウンドコールを受信するように SIP ホストのインバウンドルートを設定できます。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. [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、サードパーティーの緊急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が少なくとも1つ必要です。番号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、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 の電話番号の割り当てと割り当て解除ができます。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。

選択した数値が数値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、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. 「Call Insights」で「 をアクティブ化」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. 「部分的な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. [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 による 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 を選択します。
2. 「メディアメトリクスログ」で、「有効」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ように Voice Connector を設定する

### Note

このセクションのステップを完了するには、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 Call Analytics を使用すると、音声分析で Amazon Transcribe と Amazon Transcribe Call Analytics を使用してインサイトを自動的に生成できます。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 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「を有効化」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. [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 コールのみを処理します。グループは、フォールトトレラントな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) リージョンと米国西部 (オレゴン) リージョンの 2 つの Voice Connector を割り当てるとします。両方の Voice Connector は、SIP ホストを指す発信設定で設定します (複数可)。

次に、米国東部 (バージニア北部) リージョンの Voice Connector に着信があるとします。そのリージョンで接続に問題がある場合、通話は米国西部 (オレゴン) リージョンの Voice Connector に自動的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](#)。

## 内容

- [Amazon Chime SDK Voice Connector グループの作成](#)
- [Amazon Chime SDK Voice Connector グループの編集](#)
- [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 Voice Connector グループの削除](#)

## 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 Voice 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、グループに Voice Connector を追加します。

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に、Voice Connector ごとに異なる優先順位を入力します。1 が最優先事項です。優先度の高い Voice Connector が最初に試行されます。
6. [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、 の削除を選択します。
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 グループに電話番号を割り当てたり割り当て解除したりします。

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 1 つの 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 グループから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 に通話音声を実時間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 ストリーミングでは、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 ストリーミングでは、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、このガイドの後半にある[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。
- Voice Connector ストリーミングは、G.711 A-law および G.711  $\mu$ -law オーディオエンコーディングをサポートしています。

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 にメディアを実時間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 の通話レック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 という 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された 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、「のデータを保持」を選択し、保持期間を入力します。
7. [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



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. [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画 (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 プロトコルが 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 アドレスに送信する必要があります。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、中立のいずれかの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、以下の幅広い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、データ処理の手順を含む静的構造です。
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 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。そのためには、このガイド [通話分析を設定する](#) の「」を参照してください。作成プロセスにより、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、開始 を選択します。
5. 「分析の呼び出し」で、「を有効化」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、さまざまな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。

設定ガイドでは、各システムテストに使用される設定手順について説明します。次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 経由で SIP トランキングを有効にします。
- Voice Connector 経由で SIPREC を有効にして、オーディオストリームで使用します。

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、ポジティブ、ネガティブ、またはニュートラルのいずれかの感情を予測できます。

## トピック

- [通話分析を設定する](#)
- [通話分析の設定を使用する](#)
- [通話分析設定の更新](#)
- [通話分析設定の削除](#)
- [音声分析の有効化](#)
- [音声プロファイルドメインの管理](#)

## 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、異なる Voice Connector または異なる Amazon Kinesis Video Streams (KVS) ソースで同じ通話分析設定を使用できます。

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](#)
- [通話分析設定の作成](#)

## 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 による 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、このガイドの前半の[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 Streams。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 を作成する」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、このガイドの前半の[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。

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。

音声エンハンスメントの詳細については、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 バケットに録音された通話の音声品質を向上させるのに役立ちます。通話はナローバンドで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せん。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、通話録音が完了した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、元の録音のベース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。

音声エンハンスメントをプログラムで使用方法については、「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。

音声エンハンスメントの詳細については、<https://docs.aws.amazon.com/chime/latest/dg/> の「[音声エンハンスメントについて](#)」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、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「[分析データモデルの呼び出し](#)」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、AWS Lambda、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。アラートの詳細タイプは `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、エンドユーザーへの通知をトリガーしたり、他のカスタムビジネスロジックを開始したりできます。詳細については、このセクションで後述する「[による 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 を選択します。

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、このガイドの前半の[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。

## 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「分析の呼び出し」で「設定」を選択し、更新する設定を選択します。
3. 右上隅の[編集]を選択します。
4. 必要に応じて[通話分析を設定する](#)「」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つ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 コール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] を選択します。
4. 「設定の削除」ダイアログボックスで「」と入力 **confirm** 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。

**i 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 スピーカー検索は、発信者の音声の音声プロファイル、ベクトルマップを作成します。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

発話者検索機能では、音声埋め込みを作成します。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。デジタル埋め込み形式の生体認証情報と生体認証情報の収集、使用、保存、保持には、書面によるリリースによる発信者の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、各発信者の同意を明確に反映したプロセスを通じて、各発信者に書面によるリリースを提供する必要があります。このリリースは、サービスの使用 AWS を管理する との契約の条項で求められます。

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](#)

## 音声プロフィールドメインの作成

このセクションのステップでは、音声プロフィー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。

Amazon Chime SDK コンソールは、いずれかの制限を超えた場合にエラーメッセージを表示します。

### 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](#)。

音声プロフィー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、音声プロフィールドメイン を選択します。
3. 音声プロフィールドメインの作成 を選択します。
4. 同意確認 で、はい、Amazon Chime スピーカー検索 の同意確認 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て、タグを追加します。
7. 完了したら、音声プロフィールドメインの作成 を選択します。

## 音声プロフィールドメインの編集

作成したユーザーに関係なく、任意の音声プロフィールドメインを編集できます。



## 音声プロフィー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、音声プロフィールドメイン 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。

## 音声プロフィールドメインの削除

作成したユーザーに関係なく、任意の音声プロフィー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ィールも削除され、削除を元に戻すことはできません。

## 音声プロフィー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、音声プロフィールドメイン 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たら、削除を選択します。

## 音声プロフィー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 音声プロフィー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、値 98765 CostCenterの という名前のタグキーを作成し、そのペアをコスト配分に使用できます。音声プロフィールドメインには、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、誰が作成したかに関係なく、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。

-または-

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、誰が作成したかに関係なく、AWS アカウント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. 削除する各タグの下で 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、デジタル埋め込み形式の発話者の生体認証識別子と生体認証情報（「生体認証データ」）の収集、使用、保存、および保持には、書面によるリリースを含む発話者の同意が必要になる場合があることを了承します。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、適用法の義務および機能の使用を規定する当社のサービス条件に規定されたとおり、必要なすべての通知を各発話者に提供し、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、各発信者に書面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) で義務付けられているように、話者検索を使用する前に、各発信者の同意を明確に反映したプロセスを通じて、以下の情報を書面によるリリースとして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。発信者の音声と以前に保存した音声データを比較する目的で、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、使用することができます。このプロセスの一部として生成された生体データは、〔会社〕との最後のやり取りから最大 3 年間、または適用法で許可または要求される場合にのみより長く保持され、その後破棄されます。適用法で要求または許可されている場合を除き、〔会社〕は、データの収集または取得の最初の目的が満たされたとき、サービスとの最後のやり取りから 3 年以内、またはそのようなデータを破棄する必要があることをユーザーから通知された後のいずれか早い方までに、〔会社の〕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。生体認証データは、このサービスの提供と受信のために、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〕および Amazon Web Services が、本利用規約で説明されているとおりにお客様の生体認証データを収集、使用、および保存することを表明し、通知し、書面によるリリースおよび同意するものとします。

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、イリノイ州の各話者に対し、上記の情報を文書で提供し、実行された書面によるリリースを取得することに同意したものとみなされま

# 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](#)
- [サードパーティー緊急ルーティング番号の設定](#)
- [緊急通報での PIDF-LO の使用](#)

## 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。

このコンソールを使用して SIP ルールを作成することもできます。SIP ルールは、SIP メディアアプリケーションが Amazon Chime SDK ミーティングに接続する方法を指定します。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 またはフリーダイヤル電話番号との間で通話を行ったり来たりできます。また、Amazon Chime SDK 音声コネクタに割り当てられた名前であるリクエスト URI ホスト名との間で通話を行ったり来たりできます。Amazon Chime SDK は、ユーザーが電話をかけたり受けたりしたときに SIP ルールを実行します。SIP ルールの使用方法については、[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 ユーザーになる必要があります。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。

詳細については AWS Lambda、[「AWS Lambda の使用を開始する」](#)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

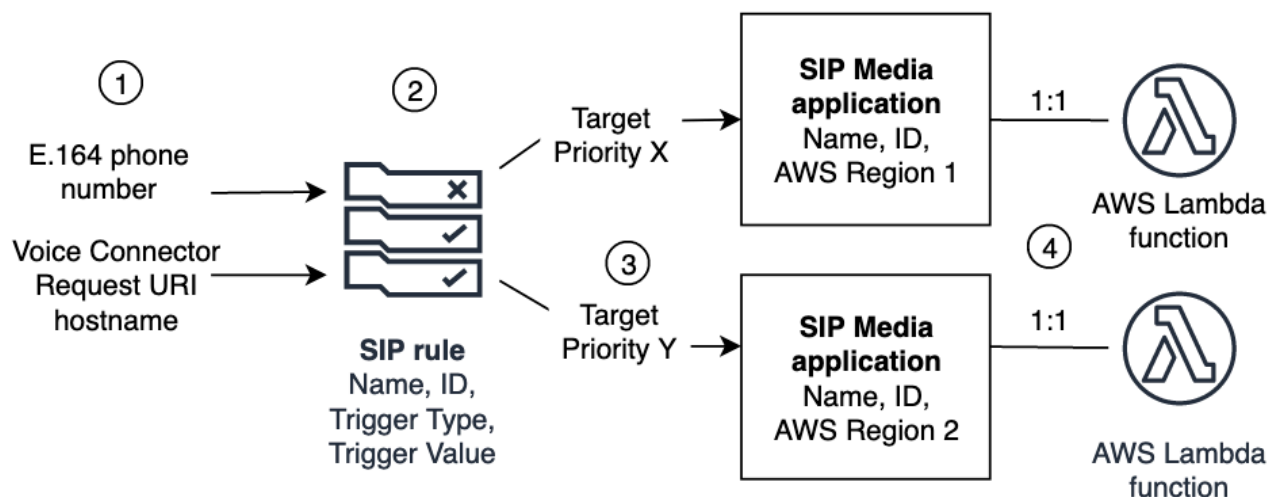
- [SIP アプリケーションとルールについて](#)
- [SIP メディアアプリケーションの使用](#)

## 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。両方とも 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。



SIP ルール (2) には、Chime インベントリと音声コネクタ (1) の電話番号のみを割り当てることができます。また、PSTN オーディオサービスで電話番号または Amazon Chime SDK 音声コネクタをプロビジョニングする必要があります。その方法については、[SIP メディアアプリケーションの作成](#)の手順で説明しています。電話番号への呼び出しを受信すると、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 (4) を呼び出します。Lambda 関数は、保留中の音楽の再生、会議への参加、通話をミュートする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実現するために、SIP ルール (2) では、フェイルオーバーの優先順位に従って、AWS 異なるリージョン (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すると、PSTN Audio サービスは次のターゲットを試みます。代替ターゲットはそれぞれ異なるリージョンに存在しなければならないことに注意してください。

AWS

# 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 AWS Lambda ルールからターゲット機能に値を渡す管理対象オブジェクトです。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前に、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でのタグの使用](#)
- [SIP メディアアプリケーションの表示](#)
- [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削除](#)

## 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を作成するのは、リクエスト URI ホスト名、Amazon Chime SDK 音声コネクタグループ、またはプライベート電話番号との間の通話と着信を有効にする必要がある場合です。

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> 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 [PSTN Audio] で [SIP メディアアプリケーション] を選択し、表示されたページで [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. 次の値のいずれかをコピーして 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 関数のバージョンのARN

#### Note

Lambda 関数を構築するときに、エイリアス ARN とバージョン ARN を作成できません。Lambda 同時実行を有効にする場合は、エイリアス ARN またはバージョン ARN が必要です。[Lambda 関数エイリアス、バージョンエイリアス、同時実行の詳細については、『開発者ガイド』の「Lambda 関数エイリアス」、「Lambda 関数バージョン」、および「Lambda プロビジョニング同時実行の管理」を参照してください。](#) [AWS Lambda](#)

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、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。 1.

[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 AWS メディアアプリケーションなどの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、リソースまたはそのリソースに保持されているデータに関する情報を格納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。たとえば、CostCenter という値を持つ名前のタグキーを作成し、そのペアをコスト配分に使用できます。98765 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](#)
- [タグを編集する](#)
- [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せん。

タグを追加するには

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 [PSTN オーディオ] 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. [Add new tag] 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 [Add new tag] 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。

## タグを編集する

必要な権限があれば、誰がタグを作成したかに関係なく、AWS アカウント内のすべてのタグを編集できます。ただし、IAM ポリシーにより編集が禁止されている場合があります。

タグを編集するには

1. <https://console.aws.amazon.com/chime-sdk/home> 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 [PSTN オーディオ] 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] ボックスまたは [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

必要な権限があれば、誰がタグを作成したかに関係なく、AWS アカウント内のタグをすべて削除できます。ただし、IAM ポリシーにより削除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> 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 [PSTN オーディオ] 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. [変更を保存] を選択します。

## 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> 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、[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 (ARN) を更新できます。リージョンは更新できません。AWS

## 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> 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、[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、以下を変更してください。
  - 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。タグの変更に関する詳細については、以下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 ARN とバージョン ARN 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 ARN またはバージョン ARN が必要です。[Lambda 関数エイリアス、バージョンエイリアス、同時実行の詳細については、『開発者ガイド』の「Lambda 関数エイリアス」、「Lambda 関数バージョン」、および「Lambda プロビジョニング同時実行の管理」を参照してください。](#) [AWS Lambda](#)

6. [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> 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、[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] を選択します。

[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。

# 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 ルールの表示](#)
- [SIP ルールの更新](#)
- [SIP ルールの有効化](#)
- [SIP ルールの無効化](#)
- [SIP ルールの削除](#)

## 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、**+110 ####**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宛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) AWS とその他のサービスを使用します。ファイアウォールがポート TCP/443 をブロックしている場合、次のサービスの許可リストに追加するか、[AWS IP アドレス範囲をに追加する必要があります](#)。\* .amazonaws.com AWS 全般のリファレンス

- Amazon EC2
- Amazon CloudFront
- Amazon Route 53

## 共通

ご使用の環境で Amazon Chime SDK を実行する場合、以下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 音声コネクタを使用する場合は、以下の宛先とポートが推奨されます。

## 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

## キャリア、メディアデスティネーション、ポート向けの Amazon ボイスフォーカス

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 が提供するメディアには、以下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 音声コネクタ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

次の表に、2022年3月以降のAmazon Chime SDK 管理ガイドの重要な変更点を示します。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 フィードをサブスクライブしてください。

変更	説明	日付
<a href="#">Alexa のスキル内通話が削除されました</a>	Amazon Alexa チームによる変更により、SIP メディアアプリケーションに Alexa コールを追加できなくなります。詳細については、「 <a href="#">Alexa スマートプロパティ</a> 」ページを参照してください。	2024年4月1日
<a href="#">サービスにリンクされたロールポリシーの更新</a>	がサービスダッシュボードで使用するメトリクスを提供 CloudWatch できるようにする AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy 追加アクセス許可。詳細については、「 <a href="#">Amazon Chime SDK メディアパイプラインでのロールの使用</a> 」および「 <a href="#">AWS 管理ポリシー</a> 」を参照してください。 AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy	2023年12月8日
<a href="#">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</a>	Kinesis Video Streams が Amazon Chime SDK 会議にオーディオ、ビデオ、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 AmazonChimeSDKMediaPipeline	2023年9月25日

sServiceLinkedRole Policy 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」](#)および[「AWS 管理ポリシー: AmazonChimeSDKMediaPipelinesServiceLinkedRole Policy」](#)を参照してください。

### [音声エンハンスメント](#)

管理者は、PSTN コールのオーディオ品質を向上させる機能である通話有効化音声エンハンスメントを有効にできるようになりました。詳細については、[「通話分析設定の作成」](#)の「音声エンハンスメントについて」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 追加されたアクセス許可。Amazon Chime Voice Connector では、メディアインサイトパイプラインの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、[AmazonChime 「SDKEvents 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 AmazonChimeVoiceConnectorServiceLinkedRolePolicy 名前を追加しました。詳細については、「[の使用 AmazonChimeVoiceConnectorServiceLinkedRole Policy](#)」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ように Voice Connector を設定する](#)」を参照してください。

2023 年 3 月 27 日

## [セキュリティポリシーの更新](#)

[AWS マネージド Amazon Chime SDK ポリシー](#)に、[Amazon Chime SDK メディアパイプライン 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 のスキル内通話](#)

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ます。この機能は削除されました。

2022 年 11 月 18 日

<a href="#">緊急 911 呼び出しを更新</a>	緊急通報プロセスを更新しました。詳細については、「 <a href="#">緊急通報の設定</a> 」を参照してください。	2022 年 8 月 4 日
<a href="#">新しいサービスにリンクされたロール</a>	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 ミーティング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、「 <a href="#">AWS マネージドポリシー: AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy</a> 」を参照してください。	2022 年 4 月 26 日
<a href="#">「Amazon Chime SDK 管理ガイド」の公開</a>	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、「 <a href="#">Amazon Chime 管理者ガイド</a> 」の「 <a href="#">Amazon Chime のドキュメント履歴</a> 」を参照してください。	2022 年 3 月 24 日

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