aws

管理ガイド

Amazon Chime

Amazon Chime: 管理ガイド

Table of Contents

このガイドのステップを完了するには、Amazon Chime システム管理者である必要があります。Amazon Chime デスクトップクライアント、ウェブアプリケーション、またはモバイルアプリに関するヘルプが必要な場合は、「Amazon Chime ユーザーガイド」の「Getting support」を参照してください。

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

Amazon Chime とは

Amazon Chime は、安全で包括的なアプリケーションを使用してオンライン会議を変革する通信サービスです。Amazon Chime は接続を維持したままデバイス間で機能します。Amazon Chime を使用して、オンライン会議、ビデオ会議、通話、チャットが可能です。組織内外のコンテンツを共有することもできます。Amazon Chime は、AWS クラウド上で安全に実行されるフルマネージドサービスであり、複雑なインフラストラクチャの展開と管理から IT 部門を解放します。

詳細については、「Amazon Chime」を参照してください。

管理の概要

管理者は、Amazon Chime コンソールを使用して、Amazon Chime アカウントの作成やユーザーとアクセス許可の管理などの主なタスクを実行します。Amazon Chime コンソールにアクセスして Amazon Chime 管理者アカウントを作成するには、まずAWS アカウントを作成する必要があります。詳細については、「Amazon Chime システム管理者の前提条件」を参照してください。

開始方法

Amazon Chime システム管理者の前提条件 の完了後、Amazon Chime 管理アカウントを作成および設定すればそこにユーザーを追加できます。ユーザーのアクセス許可 (プロまたはベーシック) を選択します。

開始する準備ができたら、次のチュートリアルを参照してください。

- はじめに

ユーザーのアクセスおよびアクセス許可の詳細については、「ユーザーアクセス許可とアクセス権の管理」を参照してください。プロアクセス許可のユーザーとベーシックアクセス許可のユーザーがアクセスできる機能の詳細については、「プランと料金表」を参照してください。

料金

Amazon Chime の料金は、使用量に応じて発生します。会議を主催するプロアクセス許可を持つユーザーに対してのみ料金が発生し、その会議を主催した日数分のみのお支払いとなります。会議の参加者とチャットのユーザーは変更されません。

ベーシックアクセス許可を持つユーザーに対して課金されることはありません。ベーシックユーザーは会議を主催できませんが、会議に参加してチャットを使用することはできます。料金およびプロアクセス許可のユーザーとベーシックアクセス許可のユーザーがアクセスできる機能の詳細については、「プランと料金表」を参照してください。

リソース

Amazon Chime の詳細については、以下の関連リソースを参照してください。

- Amazon Chime ヘルプセンター
- Amazon Chime トレーニング動画

Amazon Chime システム管理者の前提条件

Amazon Chime 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 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 管理者アカウントのセットアップを完了する方法の詳細については、「はじめに」を参照してください。

はじめに

ユーザーが Amazon Chime の使用を開始する最も簡単な方法は、30 日間無料で利用できる Amazon Chime Pro バージョンをダウンロードして使用することです。詳細については、「Amazon Chime のダウンロード」を参照してください。

Amazon Chime を購入する

30 日の無料トライアル期間を経過した後も Amazon Chime Pro バージョンを引き続き利用するには、Amazon Chime 管理者アカウントを作成して、そこにユーザーを追加する必要があります。使用を開始するには、まず「Amazon Chime システム管理者の前提条件」を完了します。ここには AWS アカウントの作成などが含まれます。その後、Amazon Chime 管理者アカウントを作成および設定し、以下のタスクを完了してユーザーを追加します。

タスク

- ステップ 1: Amazon Chime 管理者アカウントを作成する
- ステップ 2 (オプション): アカウント設定を定義する
- ステップ 3: ユーザーをアカウントに追加する
- (オプション) Amazon Chime アカウントの電話番号を設定する

ステップ 1: Amazon Chime 管理者アカウントを作成する

Amazon Chime システム管理者の前提条件 の完了後、Amazon Chime 管理者アカウントを作成できるようになります。

Amazon Chime 管理者アカウントを作成するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [アカウント] ページで、[新しいアカウント] を選択します。
3. [Account Name (アカウント名)] で、アカウントの名前を入力し、[Create account (アカウントの作成)] を選択します。
4. (オプション) Amazon Chime で、使用可能なすべてのリージョンから会議に最適な AWS リージョンが選択されるようにするか、選択したリージョンのみを使用するかを選択します。詳細については、「会議設定の管理」を参照してください。

ステップ 2 (オプション): アカウント設定を定義する

デフォルトでは、新しいアカウントはチームアカウントとして作成されます。ドメインを申請して独自の ID プロバイダーまたは Okta SSO に接続する場合は、エンタープライズアカウントに変換できます。チームアカウントタイプおよびエンタープライズアカウントタイプの詳細については、「Amazon Chime チームアカウントまたはエンタープライズアカウントのいずれかを選択する」を参照してください。

チームアカウントをエンタープライズアカウントに変換するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [アカウント] で、アカウントの名前を選択します。
3. [Identity (アイデンティティ)] で、[Getting Started (開始方法)] を選択します。
4. コンソールのステップに従って、ドメインを申請します。
5. (オプション) コンソールのステップに従って、ID プロバイダーを設定し、ディレクトリグループを設定します。

ドメインの申請の詳細については、「ドメインの申請」を参照してください。ID プロバイダーのセットアップの詳細については、「Active Directory への接続」および「Okta SSO への接続」を参照してください。

共有画面や Amazon Chime Call Me 機能のリモート制御などのオプションでアカウントポリシーを許可したり、許可を停止したりすることもできます。

アカウントポリシーを設定するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [Accounts (アカウント)] ページで、設定するアカウントの名前を選択します。
3. [設定] で、[Meetings (会議)] を選択します。
4. [ポリシー] で、許可するか、許可を停止するアカウントポリシーオプションをオンまたはオフにします。
5. [Change] を選択します。

詳細については、「会議設定の管理」を参照してください。

ステップ 3: ユーザーをアカウントに追加する

Amazon Chime チームアカウントが作成されたら、自分とユーザーを招待してチームに参加します。アカウントをエンタープライズアカウントにアップグレードする場合は、ユーザーを招待する必要はありません。その代わりに、エンタープライズアカウントにアップグレードしてドメインを申請します。詳細については、「ステップ 2 (オプション): アカウント設定を定義する」を参照してください。

ユーザーを Amazon Chime アカウントに追加するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [Accounts (アカウント)] ページで、アカウントの名前を選択します。
3. [ユーザー] ページで、[Invite users] (ユーザーの招待) を選択します。
4. 招待するユーザー (自分を含め) の E メールアドレスを入力して、[Invite users (ユーザーを招待)] を選択します。

招待されたユーザーは、作成された Amazon Chime チームアカウントに参加するための E メール招待状を受け取ります。ユーザーが Amazon Chime ユーザーアカウントを登録すると、デフォルトでプロアクセス許可が付与され、30 日間のトライアルは終了します。Amazon Chime ユーザーが既に仕事用 E メールアドレスでアカウントにサインアップしている場合、そのアカウントを引き続き使用できます。また、Amazon Chime クライアントアプリケーションは、ユーザーアカウントにサインインして [Download Amazon Chime] (Amazon Chime をダウンロード) を選択すればいつでもダウンロードできます。

プロアクセス許可を持つユーザーが会議を主催する場合にのみ料金が発生します。ベーシックアクセス許可を持つユーザーに対して課金されることはありません。ベーシックユーザーは会議を主催できませんが、会議に参加してチャットを使用することはできます。料金およびプロアクセス許可のユーザーとベーシックアクセス許可のユーザーがアクセスできる機能の詳細については、「プランと料金表」を参照してください。

ユーザーのアクセス許可を変更するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [Accounts (アカウント)] ページで、アカウントの名前を選択します。
3. [Users (ユーザー)] ページで、アクセス権限を変更するユーザーを選択します。
4. [User actions (ユーザーアクション)]、[Assign user permission (ユーザーにアクセス権限を割り当てる)] を選択します。

5. [Permissions (アクセス権限)] で、[Pro (プロ)] または [Basic (ベーシック)] を選択します。
6. [Assign (割り当てる)] を選択します。

管理者権限を持つ他のユーザーを指定し、かつ自分のアカウントの Amazon Chime コンソールへのアクセスも制御できます。詳細については、「Amazon Chime の Identity and Access Management」を参照してください。

(オプション) Amazon Chime アカウントの電話番号を設定する

Amazon Chime 管理者アカウントには、以下の電話オプションが用意されています。

Amazon Chime Business Calling

Amazon Chime との間で電話での通話やテキストメッセージを送受信できます。Amazon Chime コンソールで電話番号をプロビジョニングするか、既存の電話番号にポートインします。Amazon Chime ユーザーに電話番号を割り当てて、Amazon Chime を使用して電話での通話とテキストメッセージを送信受するためのアクセス許可を付与します。詳細については、Amazon Chime での電話番号の管理 および 既存の電話番号の移植 を参照してください。

Amazon Chime Voice Connector

既存の電話システムに SIP 追跡サービスを提供します。Amazon Chime コンソールで既存の電話番号にポートインするか、または新しい電話番号をプロビジョニングします。詳細については、「Amazon Chime SDK 管理ガイド」の「Managing Amazon Chime Voice Connectors」を参照してください。

Amazon Chime アカウントの管理

Amazon Chime は、個々のユーザーとして、または管理者のいないグループとして使用可能です。ただし、管理者機能を追加したい場合、または Amazon Chime Pro を購入したい場合には、 AWS Management Console内で Amazon Chime アカウントを作成する必要があります。Amazon Chime 管理者アカウントを作成する方法、または Amazon Chime Pro の購入の詳細については、「はじめに」を参照してください。

Amazon Chime 管理者アカウントの各種の詳細については、「Amazon Chime チームアカウントまたはエンタープライズアカウントのいずれかを選択する」を参照してください。既存の管理者アカウントの管理の詳細については、以下のトピックを参照してください。

トピック

Amazon Chime チームアカウントまたはエンタープライズアカウントのいずれかを選択する

Amazon Chime 管理者アカウントを作成する際には、チームアカウントまたはエンタープライズアカウントのどちらを作成するかを選択します。Amazon Chime 管理者アカウントの作成方法の詳細については、「はじめに」を参照してください。

チームアカウント

チームアカウントを使用すると、E メールドメインを申請しなくても、ユーザーを招待して Amazon Chime Pro のアクセス許可を付与できます。プロアクセス許可とベーシックアクセス許可の詳細については、「プランと料金表」を参照してください。

他の組織から申請されていないメールドメインからユーザーを招待できます。ユーザーの支払いは、ユーザーが会議を主催したときにのみ発生します。チームアカウントのユーザーは、Amazon Chime アプリケーションを使用して、同じアカウントに登録されている他の Amazon Chime ユーザーについて検索や連絡ができます。組織外の Pro ユーザーの支払いにもチームアカウントをお勧めします。

エンタープライズアカウント

エンタープライズアカウントを使用すると、組織のドメインからのユーザーをより細かく制御できます。独自の ID プロバイダーまたは Okta SSO に接続して、Pro または Basic のアクセス許可を認証して割り当てることができます。Amazon Chime は Microsoft Active Directory もサポートしています。

エンタープライズアカウントを作成するには、1 つ以上の E メールドメインを申請する必要があります。これにより、申請済みドメインを使用して Amazon Chime にサインインするすべてのユーザーが、一元管理されたAmazon Chime アカウントに確実に含まれるようになります。エンタープライズアカウントは、サポートされているディレクトリの統合を介してユーザーを管理するために必要です。詳細については、「ドメインの申請」および「Active Directory への接続」を参照してください。

エンタープライズアカウントからユーザーのアクティベーションや停止を管理することもできます。詳細については、「ユーザーアクセス許可とアクセス権の管理」を参照してください。

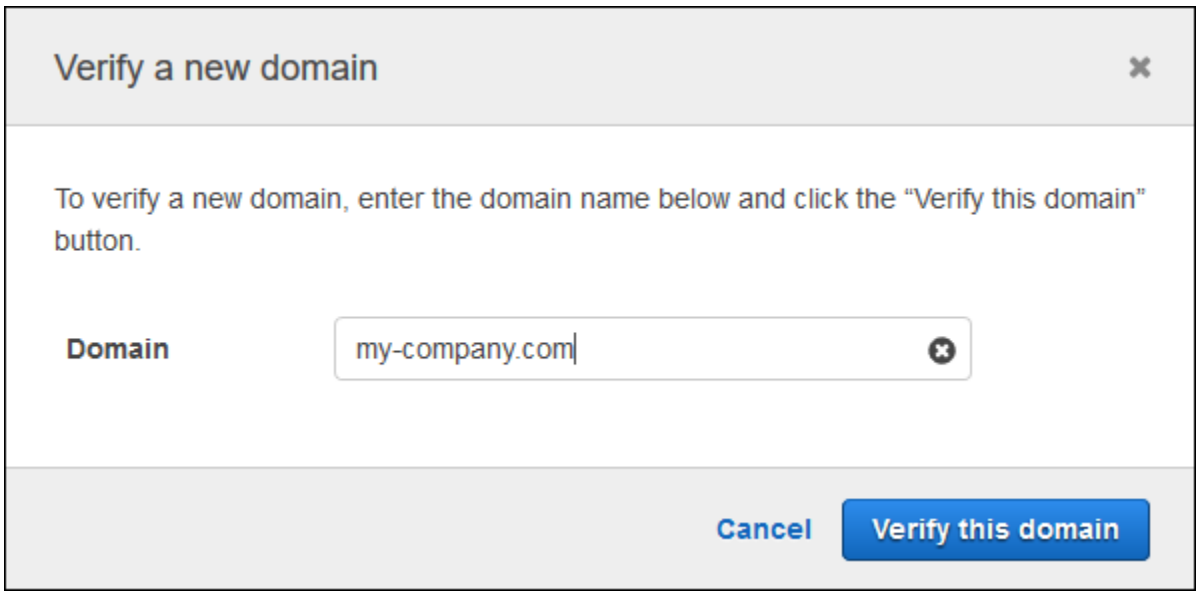
ドメインの申請

エンタープライズアカウントを作成して、このアカウントの利点であるアカウントとユーザーの強化されたコントロールを利用するには、最低 1 つの E メールドメインを申請する必要があります。

ドメインを申請するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [Accounts (アカウント)] ページで、チームアカウントの名前を選択します。

3. ナビゲーションペインで、[Identity (ID)]、[Domains (ドメイン)] の順に選択します。
4. [Domains] (ドメイン) ページで、[Claim a new domain] (新しいドメインの要求) を選択します。
5. [Domain] (ドメイン) に、組織で E メールアドレスに使用するドメインを入力します。[Verify this domain] (このドメインの検証) を選択します。



6. 画面の指示に従って、ドメインの DNS サーバーに TXT レコードを追加します。通常、このプロセスでは、ドメインのアカウントにサインインし、ドメインの DNS レコードを見つけて、Amazon Chime から提供された名前と値で TXT レコードを追加します。ドメインの DNS レコードを更新する詳しい方法については、DNS プロバイダーのドキュメントまたはドメイン名レジストラーを参照してください。

   Amazon Chime は、このレコードの有無を調べてドメインの所有者を検証します。ドメインが検証されると、そのステータスが [Pending verification] (検証中) から [Verified] (検証済み) に変わります。

   > **Note**
   >
   > DNS の変更と Amazon Chime による検証が反映されるまで最大 24 時間かかります。

7. 組織で E メールアドレスに追加のドメインやサブドメイン使用している場合は、この手順をドメインごとに繰り返します。

ドメイン申請のトラブルシューティングについての詳細は、「ドメイン申請リクエストが検証されないのはなぜですか?」を参照してください。

チームアカウントをエンタープライズアカウントに変換するには

既存のチームアカウントをエンタープライズアカウントに変換するには、Amazon Chime コンソールで 1 つ以上の E メールドメインを申請します。チームアカウントとエンタープライズアカウントの違いの詳細については、「Amazon Chime チームアカウントまたはエンタープライズアカウントのいずれかを選択する」を参照してください。ドメインの申請の詳細については、「ドメインの申請」を参照してください。

チームアカウントをエンタープライズアカウントに変換するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [アカウント] で、アカウントの名前を選択します。
3. [Identity (アイデンティティ)] で、[Getting Started (開始方法)] を選択します。
4. コンソールのステップに従って、ドメインを申請します。
5. (オプション) コンソールのステップに従って、ID プロバイダーを設定し、ディレクトリグループを設定します。

アカウントをエンタープライズアカウントに変換したら、Active Directory インスタンスを経由で接続するかどうかを決定できます AWS Directory Service。Active Directory インスタンスに接続すると、ユーザーはアクティブディレクトリの認証情報を使用して Amazon Chime にサインインできます。詳細については、「Active Directory への接続」を参照してください。

Active Directory インスタンスに接続しない場合、ユーザーは Login with Amazon ゆLWA) または Amazon.com アカウントの認証情報を使用して引き続き Amazon Chime にサインインできます。

アカウントの名前変更

以下の手順では、管理する Amazon Chime チームとエンタープライズアカウントの名前を変更する方法について説明します。選択した名前は、Amazon Chime に参加するようユーザーを招待するメールに表示されます。

アカウント名を変更するには

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

   アカウントページはデフォルトで表示されます。
2. [Account name] (アカウント名) 列で名前を変更したいアカウントを選択します。

3. 左側のペインの [Settings] (設定) の下で、[Account] (アカウント) を選択します。

   [Account summary] (アカウントの概要) ページが表示されます。
4. [Account actins] (アカウントアクション) リストを開いて [Rename account (アカウント名の変更) を選択します。

   [Rename account] (アカウント名の変更) ダイアログボックスが表示されます。
5. 新しいアカウント名を入力して [Save] (保存) を選択します。

アカウントの削除

AWS でアカウントを削除すると AWS Management Console、Amazon Chime アカウントは自動的に削除されます。または、Amazon Chime コンソールを使用して Amazon Chime チームアカウントまたはエンタープライズアカウントを削除できます。

> **Note**
>
> チームアカウントまたはエンタープライズアカウントで管理されていないユーザーは、Amazon Chime Assistant の「Delete me」コマンドを使用して削除をリクエストできます。詳細については、「Amazon Chime Assistant の使用」を参照してください。

チームアカウントを削除するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [Account name] (アカウント名) 列でアカウントを選択し、[Settings] (設定) の [Account] (アカウント) を選択します。
3. ナビゲーションペインに、[Users] (ユーザー) ページが表示されます。
4. ユーザーを選択し、[User actions] (ユーザーアクション)、[Remove user] (ユーザーの削除) の順に選択します。
5. ナビゲーションペインで、[Accounts] (アカウント)、[Account actions] (アカウントのアクション)、[Delete account] (アカウントの削除) の順に選択します。
6. アカウントを削除することを確定します。

Amazon Chime アカウントを削除するとすべてのユーザーデータが削除されます。これには、 AWS アカウント、個々の Amazon Chime アカウント、または管理対象外の Amazon Chime ユーザーの終

了が含まれます。ユーザーアカウントに関連する非コンテンツデータおよび Amazon Chime によって生成される Amazon Chime の使用状況 (カスタマーアグリーメントに含まれるサービス属性) は含まれません。

エンタープライズアカウントを削除するには

1. ドメインを削除します。

> **Note**
>
> ドメインを削除すると、以下のことが発生します。
>
> - ドメインに関連付けられていたユーザーは即時すべてのデバイスからサインアウトされ、すべての連絡先、チャット会話およびチャットルームへのアクセスが失われます。
> - このドメインからユーザーによってスケジュールされた会議は開始されなくなります。
> - 停止されたユーザーは引き続き [Users] (ユーザー) および [User detail] (ユーザー詳細) ページに [Suspended] (停止) ステータスとして表示され、そのユーザーのデータにアクセスできません。そのユーザーの E メールアドレスを使用して新しい Amazon Chime アカウントを作成することはできません。
> - 登録済みユーザーは [Users] (ユーザー) および [User detail] (ユーザー詳細) ページに [Released] (解放済み) ステータスとして表示され、そのユーザーのデータにアクセスできません。そのユーザーの E メールアドレスを使用して新しい Amazon Chime アカウントを作成することはできます。
> - Active Directory アカウントがあり、ユーザーのプライマリ E メールアドレスに関連付けられたドメインを削除した場合、ユーザーは Amazon Chime にアクセスできず、ユーザーのプロファイルは削除されます。ユーザーのセカンダリメールアドレスに関連付けられたドメインを削除すると、ユーザーはそのメールアドレスを使用してログインすることはできませんが、Amazon Chime の連絡先とデータにアクセスすることはできます。
> - エンタープライズ OpenID Connect (OIDC) アカウントがあり、ユーザーのプライマリ E メールアドレスに関連付けられたドメインを削除した場合、ユーザーは Amazon Chime にアクセスできなくなり、ユーザーのプロファイルは削除されます。

2. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
3. [Accounts (アカウント)] ページで、チームアカウントの名前を選択します。

4. ナビゲーションペインで、[Settings] (設定)、[Domains] (ドメイン) の順に選択します。
5. [Domains] (ドメイン) ページで、[Remove domain] (ドメインの削除) を選択します。
6. ナビゲーションペインで、[Accounts] (アカウント)、[Account actions] (アカウントのアクション)、[Delete account] (アカウントの削除) の順に選択します。
7. アカウントを削除することを確定します。

Amazon Chime アカウントを削除するとすべてのユーザーデータが削除されます。これには、 AWS アカウント、個々の Amazon Chime アカウント、または管理対象外の Amazon Chime ユーザーの終了が含まれます。ユーザーアカウントに関連する非コンテンツデータおよび Amazon Chime によって生成される Amazon Chime の使用状況 (カスタマーアグリーメントに含まれるサービス属性) は含まれません。

会議設定の管理

Amazon Chime コンソールから会議の設定を管理します。

会議ポリシー設定

Amazon Chime コンソールの [Settings] (設定)、[Meetings] (会議) でアカウントポリシーを管理します。次のポリシーオプションから選択します。

画面共有で共有コントロールを有効にする

所属組織のユーザーのコンピュータについて、会議中に各ユーザーが共有コントロールを許可できるかどうかを選択します。ユーザーのコンピュータの共有コントロールをリクエストした参加者は、リモートコントロールを利用できないというエラーメッセージを受け取ります。

会議への参加のためのアウトバウンド呼び出しの有効化

Amazon Chime コールミー機能をオンにします。Amazon Chime からの電話の呼び出しを受けて会議に参加するオプションを会議参加者に提供します。

会議アプリケーション設定

Amazon Chime コンソールの [Settings] (設定) の下にある [Meetings] (会議) で会議アプリケーションへのアクセスを管理します。以下のオプションを選択できます。

ユーザーが Slack 用の Amazon Chime 会議アプリケーションを使用して Amazon Chime にサインインできるようにする

このオプションを使用すると、組織内のユーザーが Slack 用の Amazon Chime 会議アプリケーションから Amazon Chime にサインインできます。詳細については、「Slack 用の Amazon Chime 会議アプリケーションを設定する」を参照してください。

会議リージョンの設定

会議の質を高め、待ち時間を短縮するために、Amazon Chime AWS はすべての参加者にとって最適なリージョンで会議を処理します。Amazon Chime で、使用可能なすべてのリージョンから会議に最適なリージョンが選択されるようにするか、選択したリージョンのみを使用するかを選択します。

この設定は、アカウントの [会議] 設定からいつでも更新できます。[Meetings] (会議) 設定から、各リージョンで処理中の Amazon Chime 会議の割合を表示することもできます。

会議のリージョン設定を更新するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [アカウント] ページで、アカウントの名前を選択します。
3. ナビゲーションペインで、[Settings (設定)]、[Meetings (会議)] の順に選択します。
4. [Regions (リージョン)] で、以下のいずれかのオプションを選択します。
   - Use all available Regions to ensure meeting quality (利用可能なすべてのリージョンを使用して会議の品質を確保する)] - Amazon Chime で会議の処理を最適化できます。
   - Use only the Regions that I select (選択したリージョンのみを使用する) – ドロップダウンメニューから、リージョンを選択できます。
5. [保存] を選択します。

チャット保持ポリシーの管理

1 つ以上の Amazon Chime エンタープライズアカウントを管理する場合、以下を対象にチャット保持ポリシーを設定できます。

- エンタープライズアカウントのメンバーのみを含むチャット会話
- エンタープライズアカウントのメンバーが作成したチャットルーム。

保持ポリシーは、設定された期間に基づいてメッセージを自動的に削除します。1 日から 15 年までの期間を設定できます。

> **Note**
>
> Amazon Chime エンタープライズアカウントの保持期間は 90 日です。このポリシーは、アカウントに属するユーザーが参加する会話、およびアカウントに属していないユーザーに適用されます。
> 保持ポリシーは以下には適用されません。
>
> - Amazon Chime エンタープライズアカウントのメンバーを含まないチャット会話
> - Amazon Chime エンタープライズアカウントに属していないユーザーが作成したチャットルーム

保持ポリシーが Amazon Chime ユーザーに与える影響

エンタープライズアカウント管理者が設定する保持ポリシーでは、ユーザーが同じエンタープライズアカウントに属しているか、別のエンタープライズアカウントに属しているか、チームアカウントに属しているか、またはどのアカウントにも属していないかによって、Amazon Chime ユーザーへの影響が異なります。

エンタープライズメンバーのチャット会話

以下の表では、保持ポリシーがエンタープライズアカウントメンバーのチャット会話にどのように影響するかを示しています。

チャット会話の参加者..。	設定される保持ポリシー..。
ユーザーのエンタープライズアカウントの他のメンバーのみ	ユーザーの管理者が設定
ユーザーのエンタープライズアカウント外の他のユーザー	自動的に 90 日に設定

エンタープライズメンバーのチャットルーム

以下の表では、保持ポリシーがエンタープライズアカウントメンバーのチャットルームにどのように影響するかを示しています。

チャットルームの作成者..。	設定される保持ポリシー..。
ユーザーのエンタープライズアカウントのメンバー	ユーザーの管理者が設定
別のエンタープライズアカウントのメンバー	他のアカウントの管理者が設定
エンタープライズアカウント外のメンバー	該当しない

チームメンバーのチャット会話

以下の表では、保持ポリシーがチームアカウントメンバーのチャット会話にどのように影響するかを示しています。

チャット会話の参加者..。	設定される保持ポリシー..。
エンタープライズアカウントのメンバーではないユーザーのみ	該当しない
エンタープライズアカウントの 1 人以上のメンバー	自動的に 90 日に設定

チームメンバーのチャットルーム

以下の表では、保持ポリシーがチームアカウントメンバーのチャットルームにどのように影響するかを示しています。

チャットルームの作成者..。	設定される保持ポリシー..。
チームアカウントのユーザー	該当しない
エンタープライズアカウントメンバーではないすべてのユーザー	該当しない
エンタープライズアカウントのメンバー	エンタープライズアカウントの管理者が設定

エンタープライズアカウントまたはチームアカウントのメンバーではない Amazon Chime ユーザーには、エンタープライズアカウントのメンバーによって作成されたチャットルームのチャットルーム保持ポリシーのみが適用されます。

エンタープライズまたはチームアカウントに属していない受取人とのチャット会話

以下の表では、保持ポリシーが Amazon Chime エンタープライズまたはチームアカウントのメンバーではないユーザーのチャット会話にどのように影響するかを示しています。

チャット会話の参加者..。	設定される保持ポリシー..。
エンタープライズアカウントのメンバーではないユーザーのみ	該当しない
エンタープライズアカウントの 1 人以上のメンバー	自動的に 90 日に設定

エンタープライズアカウントまたはチームアカウントに属していないユーザーが作成したチャットルーム

以下の表では、保持ポリシーが Amazon Chime エンタープライズまたはチームアカウントのメンバーではないユーザーのチャットルームにどのように影響するかを示しています。

チャットルームの作成者..。	設定される保持ポリシー..。
エンタープライズアカウントまたはチームアカウントのメンバーではないユーザー	該当しない
チームアカウントのユーザー	該当しない
エンタープライズアカウントのメンバー	エンタープライズアカウントの管理者が設定

チャット保持をオンにする

Amazon Chime エンタープライズアカウントの管理者は、Amazon Chime コンソールを使用して、自分のアカウントのチャット会話やチャットルームに対してチャット保持をオンにすることができます。また、コンソールを使用して、チャット保持期間を更新したり、チャット保持をいつでもオフにしたりできます。

チャット保持をオンにするには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [Accounts (アカウント)] ページで、アカウントの名前を選択します。
3. ナビゲーションペインの [設定] で [保存] を選択します。
4. 「リテンション」ページの「チャットの会話の保存」で、スライダーを「オン」 に移動します。
5. [保存期間] で、最初のボックスに数値を入力し、ボックスの横にあるリストを開いて、[日]、[週]、または [年] を選択します。
6. [チャットルームの保存] で、手順 4 ~ 5 を繰り返します。完了したら、[Save] (保存) を選択します。

保存期間を設定してから 1 日以内に、アカウントのユーザーは保存期間外に送信されたメッセージにアクセスできなくなります。

チャットメッセージの復元

> **Note**
>
> これらのステップを完了するには、Amazon Chime エンタープライズアカウント管理者である必要があります。

チャットの保存期間を設定してから 30 日以内であれば、チャットメッセージを復元できます。チャットメッセージを復元すると、Amazon Chime アカウントのすべてのユーザーが送信したすべてのメッセージが復元されます。

その 30 日以内に、次のいずれかを実行してメッセージを復元できます。

- Amazon Chime コンソールを使用してデータ保持をオフにします。

  -または-

- 保持期間を延長してください。

30 日間の猶予期間が過ぎると、保存期間に該当するチャットメッセージはすべて完全に削除されます。新しいチャットメッセージは、保存期間を過ぎるとすぐに完全に削除されます。

保存期間の設定または変更についてはチャット保持をオンにする、このセクションの前半の「」を参照してください。

また、あなたまたはアカウントメンバーが以下のいずれかのアクションを実行すると、チャットメッセージは Amazon Chime から完全に削除されます。

- Amazon Chime チャットルームを削除します。チャットルームの削除の詳細については、Amazon Chime ユーザーガイドの「チャットルームの削除」を参照してください。
- チャットメッセージが表示されている Amazon Chime ミーティングを終了します。

> **Note**
>
> 必要に応じて、会議からチャットメッセージを手動でコピーして保存できますが、その場合は会議が終了する前に行う必要があります。詳細については、Amazon Chime ユーザーガイドの「ミーティング内チャットの使用」を参照してください。

チャットメッセージを削除する

データ保持ポリシーに準拠するため、Amazon Chime はすべてのチャットメッセージを保存し、エンドユーザーが送信したメッセージを削除できないようにします。ただし、Amazon Chime システム管理者は一対の API を使用して、会話やチャットルームから個々のメッセージを削除できます。メッセージは管理者の Amazon Chime アカウントにある必要があります。

ユーザーは、メッセージ ID とそれに対応する会話またはチャットルーム ID を送信することで、メッセージの削除をリクエストできます。Amazon Chime ユーザーガイドの「チャット機能の使用」というトピックでは、その方法が説明されています。

削除リクエストを受け取ったら、コードを記述するか、 AWS CLI を使用して次の API を呼び出すことができます。

メッセージを削除するには

- 次のいずれかを行います。
  - 会話メッセージの場合 — RedactConversationMessageAPI を使用してください。

    CLI で、次のコマンドを実行します。

```
aws chime redact-conversation-message --conversation-id id_string --
message-id id_string
```

- チャットルームのメッセージの場合 — RedactRoomMessageAPI を使用してください。

  CLI で、次のコマンドを実行します。

  ```
  aws chime redact-room-message --room-id id_string --message-id
  id_string
  ```

Active Directory への接続

Amazon Chime 管理者アカウントを Active Directory に接続すると、次の機能による利点があります。

- Amazon Chime ユーザーは Active Directory 認証情報でサインインできます。
- Amazon Chime 管理者として、パスワードのローテーション、パスワードの複雑さのルール、多要素認証など、認証情報のセキュリティ機能を選択して追加できます。
- Active Directory からユーザーアカウントを削除すると、その Amazon Chime アカウントも削除されます。
- Active Directory グループを指定して Amazon Chime Pro アクセス許可を付与できます。
  - Basic または Pro アクセス許可を付与する複数のグループを設定できます。
  - Amazon Chime にサインインするには、ユーザーがいずれかのグループのメンバーであることが必要です。
  - どちらのグループのユーザーにも Pro ライセンスを付与できます。

ユーザーアクセス許可の詳細については、「ユーザーアクセス許可とアクセス権の管理」を参照してください。

前提条件

Amazon Chime でActive Directory に接続するには、以下の前提条件を満たす必要があります。

- ドメイン、アクティブディレクトリ、 AWS Identity and Access Management ディレクトリグループを設定するための正しい権限を持っていることを確認してください。詳細については、「Amazon Chime の Identity and Access Management」を参照してください。

- 米国東部 (バージニア北部) AWS Directory Service リージョンに設定されているディレクトリを作成します。詳細については、AWS Directory Service 管理ガイドを参照してください。Amazon Chime は AD Connector、Microsoft AD、または Simple AD を使用して接続を確立できます。
- Amazon Chime Enterprise アカウントを作成したり、既存のチームアカウントをエンタープライズアカウントに変換するには、ドメインを申請します。ユーザーが複数のドメインの仕事用メールアドレスを持っている場合、それらのドメインをすべて申請してください。詳細については、「ドメインの申請」および「チームアカウントをエンタープライズアカウントに変換するには」を参照してください。

Amazon Chime で Active Directory に接続する

Amazon Chime に Active Directory を接続すると、ユーザーは Amazon Chime エンタープライズアカウントで申請した各ドメインの E メールアドレスを使用する際にディレクトリの認証情報を求められます。

Amazon Chime で Active Directory に接続するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. ナビゲーションペインで、[Identity] (アイデンティティ)、[Active directory] の順に選択します。
3. [クラウドディレクトリ ID] では、Amazon Chime AWS Directory Service に使用するディレクトリを選択し、[Connect] を選択します。

   > **Note**
   >
   > ディレクトリ ID は、AWS Directory Service コンソールを使用して見つけることができます。

4. ディレクトリへの接続後に [Add a new group] (新しいグループの追加) を選択します。
5. [Group] (グループ名) にグループ名を入力します。名前は、ターゲットディレクトリの Active Directory グループと完全に一致する必要があります。Active Directory 組織単位 (OU) はサポートされていません。
6. [Permission] (アクセス許可) で、[Basic] (ベーシック) または [Pro] (プロ) を選択します。
7. [Add Group (グループの追加)] を選択します。
8. (オプション) 追加のディレクトリグループを作成するには、この手順を繰り返します。

複数の E メールアドレスの設定

Amazon Chime が Active Directory に接続すると、ユーザーは Active Directory の認証情報を使用して Amazon Chime にサインインできます。Active Directory 内では、ユーザーに複数の E メールアドレスを割り当てることができます。ユーザーが Active Directory 認証情報を使用して Amazon Chime にサインインできるようにするには、Amazon Chime 管理者アカウントで該当する各メールドメインを申請する必要があります。詳細については、「ドメインの申請」を参照してください。

> **Note**
>
> ユーザーが未申請ドメインのメールアドレスを使用してサインインしようとすると、Log in with Amazon (Amazon でログイン) でサインインするように求めるメッセージが表示されます。未申請ドメインの E メールアドレスを使用する場合、管理者アカウントにサインインすることはできません。

Amazon Chime コンソールでユーザーの詳細を表示する場合、Amazon Chime は、Active Directory から取得した `EmailAddress` 属性における単一の R メールアドレスを各ユーザーのプライマリ E メールアドレスとして使用します。これは Amazon Chime コンソールでユーザーに表示される唯一のメールアドレスです。ただし、Amazon Chime アカウント内でそれらのドメインを申請していれば、ユーザーは `ProxyAddress` 属性に列挙された追加のアドレスでサインインすることができます。

正しくない設定の例

username が shirley.rodriguez であるユーザーは、Amazon Chime アカウントのメンバーです。このアカウントでは 2 つのドメイン (example.com と example.org) が申請済みです。Active Directory 内でこのユーザーは 3 つの E メールアドレスを持っています。

- プライマリ E メールアドレス: shirley.rodriguez@example.com
- プロキシ E メールアドレス 1: shirley.rodriguez@example2.com
- プロキシ E メールアドレス 2: srodriguez@example.org

このユーザーは、shirley.rodriguez@example.com または srodriguez@example.org と shirley.rodriguez を使用して Amazon Chime にサインインできます。shirley.rodriguez@example2.com を使用してサインインしようとすると、[Amazon でログイン] でサインインするように求められ、マネージドアカウントの一部にはなりません。これが、ユーザーが E メールで使用しているすべてのドメインを申請することが重要な理由です。

他の Amazon Chime ユーザーは、shirley.rodriguez@example.com または srodriguez@example.org のいずれかの E メールアドレスを使用して、このユーザーを連絡先として追加したり、会議に招待したり、代理人として追加したりできます。

適切な設定の例

username が shirley.rodriguez であるユーザーは、Amazon Chime アカウントのメンバーです。このアカウントでは 3 つのドメイン (example.com、example2.com、および example.org) が申請済みです。Active Directory 内でこのユーザーは 3 つの E メールアドレスを持っています。

- プライマリ E メールアドレス: shirley.rodriguez@example.com
- プロキシ E メールアドレス 1: shirley.rodriguez@example2.com
- プロキシ E メールアドレス 2: srodriguez@example.org

このユーザーは、Amazon Chime にサインインするときに、どの仕事用 E メールアドレスでも使用できます。他のユーザーは、このユーザーを連絡先として追加したり、会議に招待したり、代理人として追加したりするときに、これらのいずれの仕事用 E メールアドレスでも使用できます。

Okta SSO への接続

エンタープライズアカウントを持っている場合、Okta SSO に接続して認証を行い、ユーザーにアクセス許可を割り当てることができます。

> **Note**
>
> 指定された一連の E メールアドレスドメイン内のすべてのユーザーを管理することができる、エンタープライズアカウントの作成が必要な場合は、「ドメインの申請」を参照してください。

Amazon Chime を Okta に接続するには、Okta 管理コンソールで 2 つのアプリケーションを設定する必要があります。1 つ目のアプリケーションは手動で設定され、OpenID Connect を使用してユーザーを Amazon Chime サービスに対して認証します。2 つ目のアプリケーションは、Okta Integration Network (OIN) の Amazon Chime SCIM プロビジョニングとして使用できます。これは、Amazon Chime に関する更新をユーザーやグループにプッシュするように設定されます。

Okta SSO に接続するには

1. Okta 管理コンソール で Amazon Chime アプリケーション (OpenID Connect) を作成します。
    1. [Okta Administration Dashboard (Okta 管理ダッシュボード)] にサインインしてから、[Add Application (アプリケーションの追加)] を選択します。[Create New Application (新しいアプリケーションの作成)] ダイアログボックスで、[Web (ウェブ)]、[Next (次へ)] を選択します。
    2. [Application Settings (アプリケーション設定)] を構成する
        a. アプリケーション **`Amazon Chime`** に名前を付けます。
        b. [Login Redirect URI (ログインリダイレクト URI)] に次の値を入力します。**`https://signin.id.ue1.app.chime.aws/auth/okta/callback`**
        c. [Allowed Grant Types (許可された権限のタイプ)] セクションで、それらを有効化するためのオプションをすべて選択します。
        d. [Login initiated by (ログインを開始する方法)] ドロップダウンメニューで、[Either (Okta or App) (Okta または App のいずれか)] を選択し、関連するオプションをすべて選択します。
        e. [Initiate Login URI (ログイン開始 URI)] に以下の値を入力します。**`https://signin.id.ue1.app.chime.aws/auth/okta`**
        f. [保存] を選択します。
        g. ステップ 2 で [Client ID (クライアント ID)]、[Client secret (クライアントのシークレット)]、[Issuer URI (発行者 URI)] 情報が必要になるため、このページは開いたままにしておいてください。
2. Amazon Chime コンソールで、以下の手順にし従います。
    1. [Okta single-sign on configuration (Okta シングルサインオン設定)] ページで、ページ上部から [Set up incoming keys (受信キーの設定)] を選択します。
    2. [Setup incoming Okta keys (受信 Okta キーの設定)] で、以下を入力します。
        a. [Okta Application Settings] (Okta アプリケーション設定) から [Client ID] (クライアント ID) と [Client secret] (クライアントシークレット) の情報を貼り付けます。
        b. [Okta API] ページから適切な発行元 URI を貼り付けます。[Issuer URI (発行者 URI)] は、`https://example.okta.com` などの Okta ドメインであることが必要です。
3. Okta 管理コンソールで Amazon Chime SCIM プロビジョニングアプリケーションを設定して、Amazon Chime と特定の ID およびグループメンバーシップ情報を交換します。

1. [Okta Administration Console] (Okta 管理コンソール) で、[Applications] (アプリケーション)、[Add Application] (アプリケーションの追加) を選択し、[Amazon Chime SCIM Provisioning] を検索して、アプリケーションを追加します。

   > **Important**
   >
   > 初期セットアップ中、[Do not display application to users (ユーザーにアプリケーションを表示しない)] および [Do not display application icon in the Okta Mobile App (Okta Mobile App でアプリケーションアイコンを表示しない)] の両方を選択してから、[Done (完了)] を選択します。

2. [Provisioning (プロビジョニング)] タブで、[Configure API Integration (API 統合を設定する)] を選択し、[Enable API Integration (API 統合を有効にする)] を選択します。このページは開いたままにしておいてください。次のステップで API アクセスキーのコピーが必要になります。
3. Amazon Chime コンソールで、[Create access key] (アクセスキーの作成) を選択して API アクセスキーを作成します。それをコピーして [Configure API Integration] (API 統合の設定) ダイアログボックスの [Okta API Token] (Okta API トークン) フィールドに貼り付け、[Test the Integration] (統合をテストする) を選択してから [Save] (保存) を選択します。
4. Okta が Amazon Chime の更新に使用するアクションと属性を設定します。[Provisioning (プロビジョニング)] タブの [To App (アプリへ)] セクションの下から、[Edit (編集)] を選択し、[Enable Users (ユーザーの有効化)]、[Update User Attributes (ユーザー属性の更新)]、および [Deactivate Users (ユーザーの無効化)] を選択して、[Save (保存)] を選択します。
5. [Assignments (割り当て)] タブで、新しい SCIM アプリにユーザーアクセス許可を付与します。

   > **Important**
   >
   > ライセンスに関わらず、Amazon Chime にアクセス可能なすべてのユーザーを含むグループを介してアクセス許可を付与することをお勧めします。グループは、以前にステップ 1 でユーザー向け OIDC アプリケーションを割り当てるのに使用したグループと同じ名前である必要があります。それ以外の場合、エンドユーザーはサインインすることはできません。

6. [Push Groups] (プッシュグループ) タブで、Amazon Chime と同期するグループとメンバーシップを設定します。これらのグループは、Basic ユーザーと Pro ユーザーを区別するために使用されます。

4. Amazon Chime でディレクトリグループを設定します:

   1. Amazon Chime コンソールで、[Okta single-sign on configuration] (Okta シングルサインオン設定) ページに移動します。
   2. [Directory groups (ディレクトリグループ)] で、[Add new groups (新しいグループの追加)] を選択します。
   3. Amazon Chime に追加するディレクトリグループの名前を入力します。名前は、ステップ 3-f で設定した [Push Groups (プッシュグループ)] のいずれかと完全に一致している必要があります。
   4. このグループのユーザーが [Basic (ベーシック)] または [Pro (プロ)] 機能を受け取るかどうかを選択し、[Save (保存)] を選択します。追加のグループを設定するには、このプロセスを繰り返します。

      > **Note**
      >
      > グループが見つからないというエラーメッセージが表示された場合は、2 つのシステムは同期を完了していない可能性があります。数分後に、もう一度 [Add new groups (新しいグループの追加)] を選択してください。

ディレクトリグループのユーザーの [Basic] (ベーシック) または [Pro] (プロ) 機能を選択すると、Amazon Chime エンタープライズアカウントのユーザーのライセンス、機能、コストに影響します。詳細については、「 の料金」を参照してください。

Outlook 用 Amazon Chime アドインをデプロイする

Amazon Chime は Outlook 用 に 2 つのアドインを提供しています。Windows の Outlook 用 Amazon Chime アドインと Microsoft Outlook 用 Amazon Chime アドインです。これらのアドインは同じスケジュール機能を提供しますが、異なるタイプのユーザーをサポートします。オンプレミスの Microsoft Exchange 2013 以降を使用する Microsoft Office 365 登録者および組織は、Outlook 用 Amazon Chime アドインを使用できます。Exchange サーバー 2010 以前を実行しているオンプレミスの Exchange サーバーを使用している Windows ユーザーおよび Outlook 2010 ユーザーは、Windows の Outlook 用 Amazon Chime アドインを使用する必要があります。

Outlook 用 Amazon Chime アドインをインストールする権限がない Windows ユーザーは、Windows の Outlook 用 Amazon Chime アドインを選択する必要があります。

お客様と所属する組織に適切なアドインの詳細については、「適切な Outlook アドインの選択」を参照してください。

組織に Outlook 用 Amazon Chime アドインを選択する場合、一元化されたデプロイでユーザーにこのアドインをデプロイできます。詳細については、「管理者向け Outlook 用 Amazon Chime アドインインストールガイド」を参照してください。

Slack 用の Amazon Chime 会議アプリケーションを設定する

Slack 組織を所有または管理していて Slack エンタープライズグリッド組織を使用する場合、組織の Slack 用の Amazon Chime 会議アプリケーションを設定できます。Slack ワークスペース管理者は、ご使用のワークスペースに Slack 用の Amazon Chime 会議アプリケーションを設定できます。

以下では、両方の設定方法、およびワークスペースを組織に移行するなどの追加タスクを実行する手順を説明します。

トピック

- 組織に Slack 用の Amazon Chime 会議アプリケーションをインストールする
- ワークスペースに Slack 用の Amazon Chime 会議アプリケーションをインストールする
- ワークスペースを組織に移行する
- ワークスペースを Amazon Chime チームアカウントに関連付ける

組織に Slack 用の Amazon Chime 会議アプリケーションをインストールする

Slack 用の Amazon Chime 会議アプリケーションを Slack 組織にインストールすると、ユーザーはその組織内のワークスペース内の他のユーザーとのインスタント会議や通話を開始できます。また、ワークスペース管理者は、新しいワークスペースに Slack 用の Amazon Chime 会議アプリケーションを自動的にインストールできます。以下では、その手順を説明します。

> **Note**
>
> 以下の手順では、自分が組織の所有者または管理者であり、Slack 管理コンソールにログインできることを前提としています。

組織に Slack 用の Amazon Chime 会議アプリケーションを設定する

1. Slack マネジメントコンソールの左側のペインで、[Apps] (アプリケーション) を選択します。

   [Apps] (アプリケーション) ページが開き、組織にインストールされているアプリケーション (存在する場合) が一覧表示されます。

2. ページの右上にある [Manage Apps] (アプリケーションの管理) をクリックしてから [Install an app] (アプリケーションのインストール) を選択します。

   [Find an app to install] (インストールするアプリケーションを検索) ダイアログボックスが表示されます。

3. **`Amazon Chime Meetings`** について検索してから検索結果でそれを選択します。

   [Add Amazon Chime Meetings to workspaces] (Amazon Chime 会議をワークスペースに追加する) ダイアログボックスに組織内のワークスペースが一覧表示されます。

4. Slack 用 Amazon Chime 会議アプリケーションのインストール先になる 1 つ以上のワークスペースを選択します。

5. オプションとして、すべての新しいワークスペースに Slack 用の Amazon Chime 会議アプリケーションを自動的にインストールしたい場合には [Default for future workspace] (将来のワークスペースのデフォルト) を選択してから [Next] (次へ) を選択します。

   [Review this app's requested permissions] (このアプリケーションがリクエストしたアクセス許可を確認する) ダイアログボックスが開いて Slack 用の Amazon Chime 会議アプリケーションのアクセス許可とアクションが表示されます。

6. [次へ] をクリックします。

7. 新しいワークスペースにデフォルトで Slack 用の Amazon Chime 会議アプリケーションをインストールするオプションを選択した場合、[I'm ready to set this app as a default for future workspaces] (このアプリケーションを将来のワークスペースのデフォルトとして設定する準備ができました) を選択してから [Save] (保存) を選択します。問題がなければ [Save] (保存) を選択します。

> **Note**
>
> OAuth を使用して、組織内でアプリケーションをインストールすることもできます。詳細については、Slack ヘルプの「OAuth を使用したインストール」を参照してください。

ワークスペースに Slack 用の Amazon Chime 会議アプリケーションをインストールする

Slack 用の Amazon Chime 会議アプリケーションをワークスペースにインストールすると、ユーザーはワークスペース内の他のユーザーとのインスタント会議や通話を開始できます。ユーザーが Slack 用の Amazon Chime 会議アプリケーションを使用する際に Amazon Chime ユーザープロファイルは必要ありません。Slack ユーザープロファイルを使用してログインすれば、いつでも通話や会議を開始できます。ユーザーが他の複数のユーザーとの会議を開催する必要がある場合、Amazon Chime チームアカウントを設定し、それらの追加ユーザーにPro アクセス許可を付与する必要があります。Amazon Chime の通話と会議の開始方法の詳細については、Amazon Chime ユーザーガイド「Slack 用の Amazon Chime 会議アプリケーションを使用する」を参照してください。Amazon Chime チームアカウントの設定の詳細については、このガイドの「ワークスペースを Amazon Chime チームアカウントに関連付ける」を参照してください。

Slack ワークスペース用の Amazon Chime 会議アプリケーションをインストールするには

1. Slack アプリケーションディレクトリに移動して Amazon Chime 会議アプリケーションを見つけます。
2. [Slack に追加] を選択して、Slack アプリケーションディレクトリから Amazon Chime Meetings App for Slack をインストールします。
3. Slack ワークスペースの [Calls] (通話) 設定で [Enable calling in Slack, using Amazon Chime (Amazon Chime を使用して Slack での呼び出しを有効にする) を選択します。

ワークスペースを組織に移行する

Slack 組織を所有している場合、ワークスペースをその組織に移行できます。ワークスペースの移行の詳細については、Slack ヘルプの「ワークスペースをエンタープライズグリッドに移行する」を参照してください。

ワークスペースを Amazon Chime チームアカウントに関連付ける

ワークスペースを Amazon Chime チームアカウントに関連付けて、ユーザーのアクセス許可を管理します。会議ホストを Amazon Chime Pro にアップグレードして、最大 250 人の参加者と 25 のビデオタイルで会議を開始し、音声用にダイヤルインする電話番号を含めることができます。ユーザーに Amazon Chime 基本アクセス権限を割り当てて、 one-on-one ユーザーがミーティングを開始したり、Amazon Chime ミーティングに参加したりできるようにします。詳細については、「Amazon Chime 料金表」を参照してください。

> **Note**
>
> Amazon Chime チームアカウントを Slack ワークスペースに関連付けると、ユーザーは Amazon Chime から Slack 用の Amazon Chime 会議アプリケーションにサインインできます。この設定はいつでも変更できます。詳細については、「会議設定の管理」を参照してください。

Slack ワークスペースを Amazon Chime Team アカウントに関連付ける前に、 AWS アカウントを作成する必要があります。 AWS アカウントの作成方法の詳細については、「」を参照してください。Amazon Chime システム管理者の前提条件

Slack 用の Amazon Chime 会議アプリケーションのインストール時に Slack ワークスペースを Amazon Chime チームアカウントに関連付けるには

1. Amazon Chime Meetings App を Slack ワークスペースにインストールした直後に、[Upgrade now] (今すぐアップグレード) を選択します。
2. プロンプトに従い、 AWS アカウント認証情報を使用して Amazon Chime コンソールにサインインします。
3. 画面の指示に従って、Amazon Chime で新しいチームアカウントを作成するか、既存のアカウントを選択します。

   - Create a new account (新しいアカウントを作成する) – Slack ユーザーを招待する新しい Amazon Chime アカウントを作成します。アカウント名を入力し、Slack ユーザーを招待するかどうかを選択して、[作成] を選択します。
   - Choose an existing account (既存のアカウントを選択する) – Slack ユーザーを招待する既存の Amazon Chime アカウントを選択します。アカウントを選択し、[招待] を選択します。

Slack ユーザーを Amazon Chime への参加に招待すると、E メールで招待状が届きます。招待を受け入れると、自動的に Amazon Chime Pro にアップグレードされます。

Slack 用の Amazon Chime 会議アプリケーションのインストール時に Slack ワークスペースを Amazon Chime チームアカウントに関連付けなかった場合、以下の手順を使用して後から行うことができます。

Slack 用の Amazon Chime 会議アプリケーションをインストールした後で Slack ワークスペースを Amazon Chime チームアカウントに関連付けるには

1. アカウントにサインインします。 AWS
2. 管理者として Slack ワークスペースにサインインします。
3. https://signin.id.ue1.app.chime.aws/auth/slack?purpose=app_authz に移動します。
4. プロンプトに従って、Amazon Chime で新しいチームアカウントを作成するか、既存のアカウントを選択します。

   - Create a new account (新しいアカウントを作成する) – Slack ユーザーを招待する新しい Amazon Chime アカウントを作成します。アカウント名を入力し、Slack ユーザーを招待するかどうかを選択して、[作成] を選択します。
   - Choose an existing account (既存のアカウントを選択する) – Slack ユーザーを招待する既存の Amazon Chime アカウントを選択します。アカウントを選択し、[招待] を選択します。

ユーザーの管理

> **Note**
>
> このセクションの手順は、ユーザーのメールアドレスが設定されているか、管理者アカウントを Active Directory に接続していることを前提としています。詳細については、本ガイドの Active Directory への接続「」を参照してください。

Amazon Chime コンソールを使用して、ユーザーを追加および管理します。ユーザーを招待して追加します。ユーザーが招待状を受け入れると、招待主の画面で [Users] (ユーザー) の下にアカウント内のすべてのユーザーとそのユーザー詳細が表示されます。詳細については、「ユーザー詳細の表示」を参照してください。

また、Login with Amazon (Amazon としてログイン) (LWA) を使用しているアカウントの管理者には、アクセス許可の階層の管理や、アカウントからのユーザーの削除を行うためのオプションが表示されます。これらのアクションは、使用するアカウントを構成するアクションに応じて、Active Directory または Okta を介して管理されます。詳細については、「ユーザーアクセス許可とアクセス権の管理」を参照してください。

コンテンツ

ユーザーの追加

アカウントに参加するように招待することでユーザーを Amazon Chime アカウントに追加します。Amazon Chime コンソールから潜在的なユーザーに招待を送信する手順を以下で説明します。

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

   管理しているアカウントのリストが表示されます。
2. メンバーの追加先になるアカウントを選択してから [Invite users] (ユーザーの招待) を選択します。

   [Invite new users] (新しいユーザーの招待) ダイアログボックスが表示されます。
3. 招待したいユーザーの E メールアドレスを入力します。アドレスをセミコロン (;) で区切って列記します。
4. [Invite users (ユーザーの招待)] を選択します。

新しいユーザーがリストに表示されます。ユーザーをチームアカウントに招待した場合、招待を受け入れるまでそのユーザーの詳細は表示されません。

ユーザー詳細の表示

Amazon Chime コンソールでは、[Users] (ユーザー) の下に、アカウント内のすべてのユーザーのリストが表示され、ユーザーの詳細を確認できます。E メールアドレスで特定のユーザーを検索し、ユーザーの名前を選択してユーザーの詳細を表示します。[User details] (ユーザーの詳細) の下で、ユーザーに関する詳細情報を確認し、ユーザーアカウントを更新できます。

次の表は、コンソールに表示されるユーザーの詳細を示しています。

> **Note**
>
> チームアカウントユーザーの場合、招待を受け入れるまで、完全なユーザーの詳細は表示されません。

フィールド	説明	例
Display name (表示名)	Amazon Chime に表示されるユーザーの名前。Login with Amazon (LWA) ユーザーの場合、フルネームが表示されます。Active Directory ユーザーの場合は、DISPLAY_N	Major, Mary

フィールド	説明	例
	AME_ATTRIBUTE が使用されます。	
Email address (Eメールアドレス)	LWA ユーザーの場合は、E メールアドレスを使用して登録されます。Active Directory ユーザーの場合は、Active Directory のプライマリ E メールアドレスが表示されます。	mary.major@example.com
Registration (登録)	ユーザーの現在の登録ステータスです。有効な値は、招待が送信されない場合はエンタープライズアカウント、送信される場合はチームアカウントで異なります。	[登録済み]、[Unregistered (未登録)] (チームアカウントの場合)、または [停止] (エンタープライズアカウントの場合)
Permission tier (アクセス許可の階層)	デフォルトでは [Pro] (プロ) に設定され、会議をホストできます。この項目は [ベーシック] に変更できます。	Pro (プロ)、Basic (ベーシック)
Invited (招待済み)	チームアカウントの場合、ユーザーがアカウントに招待された日付です。	2020 年 5 月 1 日
Joined (参加済み)	ユーザーが最初に Amazon Chime にサインインした日付です。Pro トライアルユーザーの場合、これは Pro トライアルの開始日でもあります。	2020 年 10 月 1 日
Personal PIN (個人用 PIN)	個人用会議 PIN。会議の設定に使用します。	0123456789

フィールド	説明	例
Privacy setting (プライバシー設定)	ユーザーが選択したプレゼンス設定。	Public (パブリック) または Private (プライベート)
Meetings attended (参加した会議)	ユーザーが参加した会議の数。	87
Meetings organized (企画した会議)	ユーザーが企画した会議の数。	12
Meeting satisfaction (会議満足度)	アンケートに対する肯定的な回答の割合。 end-of-meeting	92%
Last active date (最終アクティブ日)	ユーザーが最後にアクティブだった日付。	2020 年 6 月 12 日
Chat messages sent (送信済みチャットメッセージ数)	ユーザーが送信したチャットメッセージの数。	1025
Phone number (電話番号)	ユーザーに割り当てられた電話番号 (存在する場合)。	+12065550100

ユーザーアクセス許可とアクセス権の管理

Amazon Chime ユーザーがアクセスできる機能を管理するには、プロまたはベーシックのアクセス許可を割り当てます。ベーシックアクセス許可ユーザーは会議を主催できませんが、会議に参加してチャットを使用することはできます。プロアクセス許可ユーザーおよびベーシックアクセス許可ユーザーがアクセスできる機能の詳細については、「プランと料金表」を参照してください。

ユーザーを招待または停止することで、Amazon Chime 管理アカウントにサインインできるユーザーを管理します。ユーザーを停止できるのは、エンタープライズ管理者のみです。チームアカウント管理者は、ユーザーのアクセス許可に支払いが発生しないように、アカウントからユーザーを削除できます。ただし、サインインできないようにユーザーを停止することはできません。エンタープライズアカウントとチームアカウントの違いの詳細については、「Amazon Chime アカウントの管理」を参照してください。

ユーザーアクセス許可の管理

Amazon Chime 管理者は、Amazon Chime アカウントにおけるユーザーのプロおよびベーシックアクセス許可を管理できます。

Amazon Chime アカウントについて Active Directory または Okta を設定した場合、ユーザーアクセス許可は、グループのメンバーシップを介して管理されます。Active Directory または Okta が設定されていない場合、Amazon Chime コンソールからユーザーアクセス許可を管理してください。

チームアカウントとエンタープライズアカウントの Login with Amazon

Amazon Chime チームアカウントまたはエンタープライズの LWA アカウントを管理し、ユーザーに Login with Amazon (LWA) でサインインしてもらう場合、Amazon Chime コンソールでプロおよびベーシックアクセス許可を管理できます。

チームおよびエンタープライズ LWA アカウントのユーザーアクセス許可を管理するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [Accounts] (アカウント) で、Amazon Chime アカウントの名前を選択します。
3. [ユーザー] を選択します。
4. ユーザーを選択し、[Actions] (アクション)、[Assign permissions] (アクセス許可の割り当て) を選択します。
5. 以下のアクセス許可のいずれかを選択します。
   - Pro (プロ)
   - Basic (ベーシック)
6. [Assign (割り当てる)] を選択します。

エンタープライズ Active Directory またはエンタープライズ OpenID Connect (Okta) アカウント

ユーザーが Active Directory または Okta の認証情報を使用してサインインする場合、プロまたはベーシックアクセス許可が割り当てられているディレクトリグループにユーザーをメンバーとして加えることでアクセス許可を管理できます。

プロアクセス許可をユーザーに割り当てるには、プロアクセス許可を割り当てた Active Directory または Okta グループにユーザーをメンバーとして加えます。ベーシックアクセス許可をユーザーに割り当てるには、ベーシックアクセス許可を割り当てたグループにユーザーをメンバーとして加えま

す。プロまたはベーシックアクセス許可を持たないユーザーは Amazon Chime にサインインできません。

ユーザーアクセスの管理

Amazon Chime アカウントの管理者は、ユーザーがアカウントにサインインできるようにユーザーを招待できます。エンタープライズアカウント管理者は、ユーザーアクセスを停止して、アカウントにサインインできないようにすることができます。

チームアカウントユーザーの招待と削除

チームアカウントを管理する場合、Amazon Chime コンソールでいずれかの E メールドメインからユーザーを招待できます。

> **Note**
>
> 招待が受け入れられると、ユーザーの 30 日間トライアルは終了します。

チームアカウントにユーザーを招待するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [Accounts] (アカウント) で、チームアカウントの名前を選択します。
3. [Users] (ユーザー)、[Invite users] (ユーザーを招待) の順に選択します。
4. 招待したいユーザーの E メールアドレスを入力 (複数ある場合にはセミコロン (**;**) で区切って列記) します。
5. [Invite users (ユーザーの招待)] を選択します。

以下の手順では、割り当てられたプロアクセス許可またはベーシックアクセス許可を削除して、チームアカウントからユーザーの関連付けを解除します。削除されたユーザーは Amazon Chime にサインインできますが、Amazon Chime アカウントの有料サービスメンバーではなくなります。

チームアカウントからユーザーを削除するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [Accounts] (アカウント) で、チームアカウントの名前を選択します。
3. [ユーザー] を選択します。

4. ユーザーを選択し、[Actions] (アクション)、[Remove user] (ユーザーの削除) の順に選択します。

ユーザーに割り当てられたプロアクセス許可またはベーシックアクセス許可はすべて削除されます。ユーザーは [Contacts] (連絡先) で自動入力による新しいチームユーザーの検索ができなくなります。

エンタープライズアカウントユーザーの招待と停止

エンタープライズアカウントを管理する場合、 Amazon Chime に登録され申請済みドメインの E メールアドレスを持つすべてのユーザーが自動的にアカウントに追加されます。Active Directory または Okta を設定した場合、ユーザーは Amazon Chime 用に設定したディレクトリグループのメンバーである必要もあります。

エンタープライズアカウントにユーザーを招待するには

- 組織内のユーザーに招待状メールを送信し、Amazon Chime ユーザーガイドの「Amazon Chime アカウントの作成」の手順に従うよう指示します。

ユーザーは、アカウント用に申請されたドメインの E メールアドレスでサインインします。ユーザーが手順に従って Amazon Chime ユーザーアカウントの作成を完了すると、そのユーザーは Amazon Chime コンソールのエンタープライズアカウントの [Users] (ユーザー) の下に自動的に表示されます。

以下の手順では、Active Directory または Okta のいずれも設定されていないエンタープライズアカウントのユーザーを停止します。そうすると、ユーザーは Amazon Chime にサインインできなくなります。

エンタープライズアカウントのユーザーを停止するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [Accounts] (アカウント) で、エンタープライズアカウントの名前を選択します。
3. [ユーザー] を選択します。
4. 停止するユーザーを選択して [Actions] (アクション)、[Suspend user] (ユーザーの停止) の順に選択します。
5. チェックボックスをオンにして [Suspend] (停止) を選択します。

エンタープライズアカウント用に Active Directory または Okta を設定してある場合、以下の手順に従ってユーザーを停止します。

エンタープライズ Active Directory または OpenID Connect (Okta) アカウントのユーザーを停止するには

- 次のいずれかを行います。
  - Active Directory または Okta Administrator Dashboard から、ユーザーを停止するか、またはユーザーに非アクティブのマークを付けます。
  - ベーシックまたはプロアクセス許可が割り当てられている Active Directory グループからユーザーを削除します。

個人用会議 PIN の変更

個人用会議 PIN は、ユーザーが登録する際に生成される静的 ID です。Amazon Chime ユーザーは、この PIN を使用して、他の Amazon Chime ユーザーとの会議を簡単に設定できます。個人用会議 PIN を使用すれば、会議の主催者は、設定する新しい会議の詳細を覚えておく必要がなくなります。

個人用会議 PIN が漏洩した可能性がある場合は、PIN をリセットし、新しい ID を生成できます。個人用会議 PIN を更新したら、古い個人用会議 PIN を使用して、設定したすべての会議を更新する必要があります。

個人用会議 PIN を変更するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [Accounts] (アカウント) ページで、Amazon Chime チームアカウントの名前を選択します。
3. ナビゲーションペインで [Users (ユーザー)] を選択します。
4. PIN を変更する必要のあるユーザーを検索します。
5. [User detail] (ユーザー詳細) ページを開くには、目的のユーザーの名前を選択します。
6. [ユーザー操作]、[Reset personal PIN (個人用 PIN のリセット)]、[確認] の順に選択します。

Pro トライアルの管理

ユーザーが Amazon Chime チームの招待を受け入れるか、エンタープライズアカウントに追加されると、無料トライアルは終了し、プロアクセス許可が付与されます。これにより、ユーザーは、予定

されている会議を引き続きホストできます。ユーザーのアクセス許可の階層をベーシックに変更すると、会議ホストとして操作できなくなります。

Amazon Chime の料金表は、使用状況に基づいており、ホストした日数で会議をホストしたユーザー分のみのお支払いとなります。会議の参加者とチャットのユーザーは変更されません。

主催した会議がカレンダーの日付どおりに終了しており、次のうち 1 つ以上に該当している場合、プロユーザーは、アクティブなプロとみなされます。

- 会議が設定されていた。
- 会議に参加者が 3 人以上いた。
- 会議に複数の記録イベントが含まれていた。
- ダイヤルインした参加者が会議に含まれていた。
- 会議に H.323 または SIP を使用した参加者が含まれていた。

詳細については、「プランと料金表」を参照してください。

ユーザーの添付ファイルのリクエスト

エンタープライズアカウントを管理し、適切なアクセス許可がある場合、ユーザーが Amazon Chime にアップロードした添付ファイルをリクエストして取得できます。ユーザーが 1:1 およびグループ会話、または作成されたチャットルームにアップロードした添付ファイルを取得できます。

> **Note**
>
> Amazon Chime チームアカウントを管理している場合、1 つ以上のドメインを申請することでエンタープライズアカウントをアップグレードできます。また、ユーザーをチームアカウントから削除することもできます。こうすることで、管理対象外のユーザーは Amazon Chime Assistant を使用して添付ファイルを取得できます。

ユーザー添付ファイルをリクエストするには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [Accounts] (アカウント) ページで、Amazon Chime チームアカウントの名前を選択します。
3. [Settings] (設定) で、[Account] (アカウント)、[Account actions] (アカウントのアクション)、[Request attachments] (添付ファイルのリクエスト) の順に選択します。

4. 約 24 時間以内に、[Account summary] (アカウントの概要) ページに各添付ファイルにアクセスするために使用する署名付き URL のリストを含むファイルへのリンクが表示されます。
5. ファイルをダウンロードします。

> **Note**
>
> ファイルのアクセス制御には適切なレベルを維持してください。このファイルを取得したユーザーは誰でも、記載された URL のリストを使用して関連添付ファイルをダウンロードできます。
> 署名付き URL は、6 日後に失効します。リクエストは 7 日に 1 回送信できます。

AWS Identity and Access Management (IAM) ポリシーを使用して Amazon Chime 管理コンソールへのアクセスと添付ファイルをリクエストアクションを管理するには、Amazon Chime 管理ポリシー (FullAccess、 UserManagement、または) のいずれかを使用します。 ReadOnlyまたは、`StartDataExport` アクションおよび `RetrieveDataExport` アクションを含むようにカスタムポリシーを更新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「Amazon Chime で定義されるアクション」を参照してください。

Amazon Chime での自動更新の管理方法

Amazon Chime は、クライアントをアップデートするためのさまざまな方法を提供しています。Amazon Chime をブラウザで起動するか、デスクトップで起動するか、モバイル端末で起動するかによって、方法が異なります。

Amazon Chime のウェブアプリケーション (https://app.chime.aws) は、常に最新の機能とセキュリティフィックスでロードします。

Amazon Chime デスクトップクライアントは、[Quit] (止める) または [Sign Out] (サインアウト) を選択するたびに、アップデートを確認します。これは、Windows と macOS のマシンに適用されます。クライアントを実行すると、3 時間ごとにアップデートを確認します。また、Windows のヘルプメニューまたは macOS の Amazon Chime メニューで [Check for Updates] (更新プログラムの確認) を選択しても更新の有無を確認できます。

デスクトップクライアントがアップデートを検出すると、会議中でない限り、Amazon Chime がインストールを促します。以下のユーザーは進行中の会議に参加していることになります。

- 彼会議に出席している。

- まだ進行中の会議に招待された。

Amazon Chime は、最新バージョンをインストールするように促し、15 秒間の秒読みを開始し、インストールの延期を可能にします。ユーザーは [Try Later] (後で試す) を選択して更新を延期します。

更新を延期した場合、会議に出席していなければ、クライアントは 3 時間後に更新の有無を確認して、もう一度インストールを促します。秒読みが終了するとインストールが開始されます。

> **Note**
>
> macOS ユーザーは [Restart Now] (今すぐ再起動) を選択してアップデートを開始する必要があります。

モバイルデバイス上 - Amazon Chime モバイルアプリケーションは、App Store および Google Play が提供する更新オプションを使用して、Amazon Chime クライアントの最新バージョンを配信します。モバイルデバイス管理システムを使用して更新プログラムを展開することもできます。

ユーザーを別のチームアカウントに移行する

移行先アカウントが存在しない場合、移行先アカウントを作成して設定することによって、ユーザーをそのチームアカウントに移行します。次いで、移行先アカウントにユーザーを追加します。以下の手順に従うことで、移行の各段階の完了に関する情報が表示されます。

ユーザーを移行するには

1. 移行先アカウントがない場合、アカウントを 1 つ作成します。詳細については、「ステップ 1: Amazon Chime 管理者アカウントを作成する」を参照してください。
2. 必要に応じて、アカウントを設定します。詳細については、「ステップ 2 (オプション): アカウント設定を定義する」を参照してください。
3. アカウントにユーザーを追加します。詳細については、「ステップ 3: ユーザーをアカウントに追加する」を参照してください。

Amazon Chime での電話番号の管理

電話番号のプロビジョニングには Amazon Chime コンソールを使用します。番号をプロビジョニングするときは、Amazon Chime が管理する番号プールから番号をリクエストします。電話番号の割り当てを解除して削除すると、番号はプールに戻されます。番号を移植するときは、その番号を Amazon Chime に移植したり、Amazon Chime から移植したりします。

> **Note**
>
> Amazon Chime コンソールを使用する場合、Amazon Chime ビジネス通話番号のみをプロビジョニングできます。国際電話番号が必要な場合は、Amazon Chime 音声コネクタと SIP メディアアプリケーションを使用します。そのためには、まず Amazon Chime SDK 管理者アカウントを作成する必要があります。詳細については、Amazon Chime SDK 管理者ガイドの以下のトピックを参照してください。
>
> - 前提条件
> - 電話番号インベントリの管理
> - 音声コネクタの管理
> - SIP メディアアプリケーションの管理

以下のセクションのトピックでは、Amazon Chime 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。

コンテンツ

電話番号のプロビジョニング

Amazon Chime コンソールを使用して、Amazon Chime アカウントに電話番号をプロビジョニングします。電話番号は Amazon Chime が管理するプールから取得されます。Amazon Chime Business Calling を選択して電話番号をプロビジョニングし、既存の Amazon Chime ユーザーに割り当てます。

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] に表示されます。次にこれらの番号を個々のユーザーに割り当てます。

電話番号をプロビジョニングするには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. ナビゲーションペインで、[Calling] の [電話番号管理] を選択します。
3. [注文]、[Provision phone numbers (電話番号のプロビジョニング)] を選択します。
4. [Business Calling] を選択し、[次へ] を選択します。
5. 利用可能な電話番号を検索します。設定したい電話番号を選択してから [Provision] (プロビジョニング) を選択します。

プロビジョニングの発生中に電話番号は、[Orders] (申し込み) および [Pending (保留中) のリストに表示されます。

既存の電話番号の移植

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。

> **Note**
>
> 国際電話番号を移植したり、Amazon Chime 音声コネクタを使用したり、SIP メディアアプリケーションを使用したりする必要がある場合は、Amazon Chime SDK 管理者アカウントを作成し、Amazon Chime SDK コンソールを使用する必要があります。その方法の詳細については、Amazon Chime SDK 管理者ガイドの「前提条件」を参照してください。

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

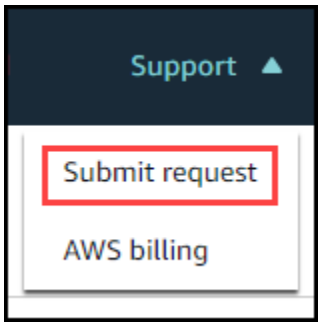
ポート番号には、機関委任状 (LOA) が必要です。国内の電話番号には LOA が必要です。エージェンシーレター (LOA) フォームをダウンロードして記入してください。異なる通信事業者の電話番号を移管する必要がある場合は、通信事業者ごとに個別の LOA を記入してください。

電話番号の移植

既存の電話番号を移植するサポートリクエストを作成します。

既存の電話番号を移植するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. ページ上部のコマンドバーで [Support] を選択し、[リクエストを送信] 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) 請求先電話番号 (BTN) を移植する場合は、以下のいずれかのオプションを選択します。
        - 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)
        - オプションを選択したら、依頼書に委任状 (LOA) を添付してください。

      国際番号を移植する場合:

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

- 番号のタイプ (市内または通話料無料)
- 持ち込もうとする既存の電話番号。
- 使用量の推定
- 国

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

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

e. [移植日] に、希望する移植日を入力します。

f. 「移植時間」に、希望する時間を入力します。

g. [次のステップ: 今すぐ解決またはお問い合わせ] を選択します。

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

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

必要書類の提出

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

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

書類を提出するには

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

2. アカウントにサインインし、 AWS アカウント専用に生成された Amazon S3 アップロードリンクを開きます。

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

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

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

リクエストステータスの表示

以下の手順では、Amazon Chime 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方法を説明します。

ステータスを表示するには

1. https://chime.aws.amazon.com/ で Amazon Chime 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

電話会社が LOA が正しいことを確認したら、要求されたポートを確認して承認します。次に、ポートが実行される確定注文コミット (FOC) AWS Support の日時を提示します。

FOC 日になると、移管された電話番号が使用可能になります。その後、その番号を目的のアカウントのユーザーに割り当てる必要があります。

電話番号を割り当てるには

1. https://chime.aws.amazon.com/ で Amazon Chime 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. 「インベントリ」タブで、割り当てる番号の横にあるチェックボックスを選択し、「割り当て」を選択します。

   > **Note**
   >
   > 一度に 1 つの番号しか選択できません。

4. 「ユーザープロファイルに +1 電話番号を割り当てる」ページで、その番号のアカウントを選択し、「次へ」を選択します。
5. 番号を割り当てるユーザーを選択し、[割り当て] を選択します。

電話番号の移植

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「Amazon Chime ビジネスコーリング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 のリクエスト方法

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://chime.aws.amazon.com/ で Amazon Chime 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。

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 に移植するリクエストを送信した後で、移植リクエストのステータスを確認するには、Amazon Chime コンソールで [Calling] (呼び出し)、[Phone number management] (電話番号管理)、[Pending] (保留中) の順に選択します。

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。

Amazon Chime ビジネスコーリング電話番号の割り当て

電話番号管理インベントリページを使用して、Amazon Chime Business Calling の電話番号を個々のユーザーに割り当てます。

Amazon Chime ビジネスコーリング電話番号を割り当てるには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. ナビゲーションペインで、[Calling] の [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ます。
4. [Assign (割り当てる)] を選択します。
5. ユーザーが所属するアカウントを選択し、[次へ] を選択します。
6. ユーザーを選択し、[Assign] を選択します。

電話番号または電話番号の権限を変更する場合は、新しい権限情報をユーザーに提供することをおすすめします。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。

Amazon Chime ビジネスコーリング電話番号の割り当て解除

次の手順に従って、Amazon Chime Business Calling ユーザーから電話番号の割り当てを解除します。

電話番号の割り当てを解除するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. ナビゲーションペインで、[Calling] の [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. [割り当て解除] を選択します。
5. 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。

インベントリ内の番号の詳細を表示できます。たとえば、電話やテキストメッセージが有効になっているかどうかを確認できます。

インベントリ電話番号の詳細を表示するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. ナビゲーションペインで、[Calling] の [電話番号管理] を選択します。
3. [インベントリ] タブを選択し、表示したい電話番号を選択します。
4. [アクション] リストを開いて [詳細を表示] を選択します。

アウトバウンドコール名を使用する

発信者名は発信者 ID として機能します。インベントリ内の 1 つまたは複数の電話番号にデフォルトの発信者名を設定できます。個々の電話番号に固有の発信者名を設定することもできます。その後、その電話番号を使用して発信された通話の受信者には、その名前が表示されます。発信者名はすべての電話番号製品タイプに適用されます。名前は 7 日に 1 回更新できます。

たとえば、その部署のすべての電話番号について、デフォルトの発信者名を部門 5 に設定できます。また、部長には Jane Doe という固有の名前を設定することもできます。

次の手順では、デフォルトコール名と個別のアウトバウンドコール名を設定する方法について説明します。

発信者名を設定するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. ナビゲーションペインで、[Calling] の [電話番号管理] を選択します。
3. 「インベントリ」タブで、次のいずれかを実行します。更新する電話番号の横にあるチェックボックスを選択します。

- 複数の電話番号にデフォルトの発信者名を設定するには、その番号の横にあるチェックボックスを選択します。
- 個別の発信者名を設定するには、希望する番号を選択します。

4. 「アクション」リストを開き、「デフォルトの発信者名を更新する」を選択します。
5. [デフォルトの発信者名] ボックスに、デフォルトの発信者名を 15 文字以内で入力します。
6. [保存] を選択します。

システムがデフォルトの発信者名を更新するまでに 72 時間かかります。

電話番号を削除する

> **Important**
>
> これらの手順を実行できるのは Amazon Chime システム管理者のみです。また、削除する前に電話番号の割り当てを解除する必要があります。

電話番号をプロビジョニングするときは、Amazon Chime が管理している番号プールに電話番号を注文します。電話番号を削除すると、その番号はプールに戻されます。電話番号を削除すると、その番号はまず削除キューに送られ、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。これで番号が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://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. ナビゲーションペインで、[Calling] の [電話番号管理] を選択します。
3. [インベントリ] タブを選択し、削除したい電話番号を選択します。
4. [アクション] リストを開いて [電話番号を削除] を選択します。
5. チェックボックスをオンにし、[削除] を選択します。

削除された電話番号は、完全に削除されるまで [削除キュー] に 7 日間保持されます。

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 [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。

削除された電話番号を復元するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. ナビゲーションペインで、[Calling] の [電話番号管理] を選択します。
3. [削除キュー] タブを選択したら、復元する 1 つ以上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。

Amazon Chime のグローバル設定の管理

Amazon Chime コンソールを使用して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 管理アカウントで通話詳細レコードを設定する前に、まず Amazon Simple Storage Service バケットを作成します。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。データを保存して管理するためには、通話詳細レコード設定を構成する際に Amazon S3 バケットへの Amazon Chime 読み書きアクセス権を付与します。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 Business Calling の通話詳細レコード設定を構成できます。Amazon Chime Business Calling の詳細については、「Amazon Chime での電話番号の管理」を参照してください。

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://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
3. [グローバル設定] で [Call detail records (通話詳細レコード)] を選択します。
4. [Business Calling の設定] を選択します。
5. [Log destination] (ログ転送先) として Amazon S3 バケットを選択します。
6. [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://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [グローバル設定] で [Call detail records (通話詳細レコード)] を選択します。
3. 該当する設定に対して [Disable logging (ログを無効にする)] を選択します。

Amazon Chime Business Calling 通話詳細レコード

Amazon Chime Business Calling の通話詳細レコードを受信するオプションを選択すると、レコードは Amazon S3 バケットに送信されます。次の例は、Amazon Chime Business Calling 通話詳細レコード名の一般形式を示しています。

```
Amazon-Chime-Business-Calling-CDRs/json/111122223333/2019/03/01/123a4567-
b890-1234-5678-cd90efgh1234_2019-03-01-17.10.00.020_1a234567-89bc-01d2-3456-
e78f9g01234h
```

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-Business-Calling-CDRs/json/awsAccountID/year/month/
day/conferenceID_connectionDate-callStartTime-callDetailRecordID
```

次の例は、Amazon Chime Business Calling 通話詳細レコードの一般形式を示しています。

```
{
    "SchemaVersion": "2.0",
    "CdrId": "1a234567-89bc-01d2-3456-e78f9g01234h",
    "ServiceCode": "AmazonChimeBusinessCalling",
    "ChimeAccountId": "12a3456b-7c89-012d-3456-78901e23fg45",
    "AwsAccountId": "111122223333",
    "ConferenceId": "123a4567-b890-1234-5678-cd90efgh1234",
    "ConferencePin": "XXXXXXXXXX",
    "OrganizerUserId": "1ab2345c-67de-8901-f23g-45h678901j2k",
    "OrganizerEmail": "jdoe@example.com",

    "CallerPhoneNumber": "+12065550100",
    "CallerCountry": "US",

    "DestinationPhoneNumber": "+12065550101",
    "DestinationCountry": "US",

    "ConferenceStartTimeEpochSeconds": "1556009595",
    "ConferenceEndTimeEpochSeconds": "1556009623",
    "StartTimeEpochSeconds": "1556009611",
    "EndTimeEpochSeconds": "1556009623",
    "BillableDurationSeconds": "24",
    "BillableDurationMinutes": ".4",
    "Direction": "Outbound"
```

```
}
```

会議室の設定

SIP または H.323 プロトコルを使用する場合、Amazon Chime は、Cisco、Tandberg、Polycom、Lifesize、Vidyo、その他の室内ビデオシステムと統合できます。

SIP をサポートする会議室 VTC デバイスを使用して Amazon Chime に接続するには、以下のいずれかのオプションを入力します。

- **@meet.chime.in**
- **u@meet.chime.in**
- 10 桁の会議 ID とそれに続く **@meet.chime.in**

meet.chime.in は、SIP ルームデバイスを最も近い Amazon Chime リージョンに接続します。特定のリージョンに接続するには、SIP ルームシステムのリージョン固有の DNS エントリを使用します。詳細については、「セッション初期化プロトコル (SIP) ルームシステム」を参照してください。

> **Note**
>
> SIP ルームデバイスが TLS をサポートしておらず、TCP 接続が必要な場合は、AWS サポートにお問い合わせください。

H.323 のみをサポートするデバイスを使用している場合は、次のいずれかにお電話ください。

- **13.248.147.139**
- **76.223.18.152**

VTC デバイスと Amazon Chime の間のトラフィックがファイアウォールでフィルタ処理される場合、使用するプロトコルの範囲を開きます。詳細については、「ネットワーク設定と帯域幅の要件」を参照してください。

Amazon Chime のようこそ画面で、参加する会議の 10 桁または 13 桁の ID を入力します。Amazon Chime クライアントまたはウェブアプリケーションで 13 桁の会議 ID を見つけるか、[Dial-in] (ダイヤルイン) オプションを選択できます。

モデレート会議への参加

参加するのがモデレート会議であり、その主催者または代理人である場合は、13 桁の会議 ID を入力し、モデレーターとして会議に参加します。モデレーターとして参加する場合、ダイヤルパッドでモデレーターパスコードを入力し、その後にポンド記号 (#) を入力して、会議に参加して開始します。主催者、代理人、またはモデレーターではない場合は、モデレーターが会議に参加して開始した後に、会議に接続されます。

モデレーターには主催者のコントロールがあります。つまり、追加の会議アクションを実行できます。これらのアクションには、記録の開始と停止、会議のロックとロック解除、他のすべての参加者のミュート、会議の終了が含まれます。詳細については、Amazon Chime ユーザーガイドの「電話または室内ビデオシステムを使用したモデレーターアクション」を参照してください。

> **Note**
>
> Alexa for Business を使用して Amazon Chime 会議に参加する場合は、デバイスが室内ビデオシステムに接続され、デバイスのダイヤルパッドを使用してダイヤルインするのであれば、モデレーターとして参加できます。

互換性のある VTC デバイス

以下の表は、互換性のある VTC デバイスリストからの抜粋です。

デバイス	SIP	H.323	コメント
Cisco SX20	はい	Yes	オーディオ/ビデオ/画面: 双方向に OK
Cisco DX80	はい	Yes	オーディオ/ビデオ/画面: 双方向に OK
Lifesize Icon	Yes	No	オーディオ/ビデオ/画面: 双方向に OK
Polycom Debut	はい	Yes	オーディオ/ビデオ/画面: 双方向に OK

デバイス	SIP	H.323	コメント
Polycom RealPresence デスクトップ	No	Yes	オーディオ/ビデオ: OK、画面: デバイスからは OK
Polycom Trio	はい	Yes	オーディオ/ビデオ/画面: 双方向に OK
Tandberg C40	はい	Yes	オーディオ/ビデオ/画面: 双方向に OK

ネットワーク設定と帯域幅の要件

Amazon Chime 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 は、ポート TCP/443 で Amazon Elastic Compute Cloud (Amazon EC2) やその他の AWS サービスを使用します。ファイアウォールでポート TCP/443 がブロックされる場合、「AWS 全般のリファレンス」に従い、以下のサービスについて許可リストに `*.amazonaws.com` を追加するか、AWS IP アドレス範囲を設定する必要があります。

- Amazon EC2
- Amazon CloudFront
- Amazon Route 53

宛先、ポート、帯域幅の詳細については、以下のセクションを参照してください。

必要な宛先とポート

Amazon Chime を実行するには、以下のデスティネーション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
*.chime.aws	TCP/443
*.amazonaws.com	TCP/443
99.77.128.0/18	TCP/443

ミーティングポートとテレフォニーポート

Amazon Chime では、会議や Amazon Chime ビジネス通話に次の送信先とポートを使用します。

デスティネーション	ポート
99.77.128.0/18	UDP:3478

H.323 ルームシステム

Amazon Chime では、H.323 室内ビデオシステムに次の送信先とポートを使用します。

デスティネーション	ポート
13.248.147.139	TCP/1720
76.223.18.152	TCP/1720
99.77.128.0/18	TCP/5100:6200
34.212.95.128/25	UDP/5100:6200
34.223.21.0/25	
52.55.62.128/25	
52.55.63.0/25	

セッション初期化プロトコル (SIP) ルームシステム

ご使用の環境で SIP 室内ビデオシステムに Amazon Chime を実行する場合は、次の宛先とポートをお勧めします。

AWS 地域	デスティネーション	ポート
グローバル (最も近いリージョン)	99.77.128.0/18	UDP/10000:60000
	34.212.95.128/25	
	34.223.21.0/25	
	52.55.62.128/25	

AWS 地域	デスティネーション	ポート
	52.55.63.0/25	
グローバル	meet.chime.in 13.248.147.139 76.223.18.152	TCP/5061
米国東部 (バージニア北部)	meet.ue1.chime.in	TCP/5061
米国西部 (オレゴン)	meet.uw2.chime.in	TCP/5061
アジアパシフィック (シンガポール)	meet.as1.chime.in	TCP/5061
アジアパシフィック (シドニー)	meet.as2.chime.in	TCP/5061
アジアパシフィック (東京)	meet.an1.chime.in	TCP/5061
欧州 (アイルランド)	meet.ew1.chime.in	TCP/5061
南米 (サンパウロ)	meet.se1.chime.in	TCP/5061

帯域幅の要件

Amazon Chime のオーディオ、ビデオ、および画面共有の帯域幅要件は以下のとおりです。

- 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
- 画面共有
    - 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

レポートの表示

十分な知識に基づく意思決定し、組織の生産性を向上させるために、使用状況とフィードバックのデータには、コンソールから直接アクセスできます。レポートデータは毎日更新されますが、最大 48 時間の遅延が生じることがあります。

使用状況とフィードバックレポートを表示するには

1. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
2. [レポート]、[ダッシュボード] を選択します。
3. [Usage and feedback dashboard report] (使用状況とフィードバックダッシュボードレポート) ページで、次のデータを表示します。

> **Note**
>
> 利用可能なデータについては、「Amazon Chime レポートダッシュボードとユーザーアクティビティの詳細」を参照してください。

- Date range (UTC) (日付範囲 (UTC)) — レポートの日付範囲。
- Registered users (登録ユーザー) — Amazon Chime にサインアップしたユーザーの数。
- Active users (アクティブなユーザー) — Amazon Chime で会議に出席するかメッセージを送信したユーザーの数。
- Meetings held (開催された会議) — 終了した会議の合計数。特定の会議を選択すると、会議 ID、開始時刻、種類、主催者、期間、および出席者数などの、詳細を表示できます。特定の [Conference ID] (会議 ID) または [Meeting organizer] (会議の主催者) 値を選択して、出席者、会議名簿イベント、クライアントの種類、および会議のフィードバックを含む追加の詳細を表示します。
- Meeting satisfaction (会議満足度) — 会議終了時に提出されたアンケートの賛成数の割合。
- Chat messages sent (送信済みチャットメッセージ) — ユーザーがチャットで送信したメッセージの数。

Amazon Chime デスクトップクライアントの拡張

チャットボット、プロキシ電話セッション、ウェブフックを追加して、Amazon Chime デスクトップクライアントの機能を拡張できます。チャットボットを使用すると、ユーザーは内部システムの情報のクエリなどのタスクを実行できます。プロキシ電話セッションを使用すると、ユーザーは電話番号を公開せずに電話をかけたりテキストメッセージを送信したりできます。ウェブフックは、チャットルームに自動的にメッセージを送信できます。例えば、ウェブフックは会議へのリンクと共に会議のリマインダーをチームに送信できます。

トピック

ユーザー管理

次のコードスニペットは、Amazon Chime ユーザーの管理に役立ちます。このトピックの例はすべて Java を使用しています。

トピック

複数ユーザーの招待

次の例は、Amazon Chime Team アカウントに複数のユーザーを招待する方法を示しています。

```
List<String> emails = new ArrayList<>();
emails.add("janedoe@example.com");
emails.add("richardroe@example.net");
InviteUsersRequest inviteUsersRequest = new InviteUsersRequest()
    .withAccountId("chimeAccountId")
    .withUserEmailList(emails);
```

```
chime.inviteUsers(inviteUsersRequest);
```

ユーザーリストのダウンロード

次の例は、Amazon Chime 管理アカウントに関連付けられているユーザーのリストを .csv 形式でダウンロードする方法を示しています。

```
BufferedWriter writer = Files.newBufferedWriter(Paths.get("/path/to/csv"));
CSVPrinter printer = new CSVPrinter(writer, CSVFormat.DEFAULT.withHeader("userId",
 "email"));

ListUsersRequest listUsersRequest = new ListUsersRequest()
    .withAccountId(accountId)
    .withMaxResults(1);

boolean done = false;
while (!done) {
    ListUsersResult listUsersResult = chime.listUsers(listUsersRequest);
    for (User user: listUsersResult.getUsers()) {
        printer.printRecord(user.getUserId(), user.getPrimaryEmail());
    }

    if (listUsersResult.getNextToken() == null) {
        done = true;
    }

    listUsersRequest = new ListUsersRequest()
        .withAccountId(accountId)
        .withNextToken(listUsersResult.getNextToken());
}

printer.close();
```

複数ユーザーのログアウト

次の例は、Amazon Chime 管理者アカウントから複数のユーザーをログアウトする方法を示しています。

```
ListUsersRequest listUsersRequest = new ListUsersRequest()
    .withAccountId("chimeAccountId");
```

```
ListUsersResult listUsersResult = chime.listUsers(listUsersRequest);

for (User user: listUsersResult.getUsers()) {
    LogoutUserRequest logoutUserRequest = new LogoutUserRequest()
        .withAccountId(user.getAccountId())
        .withUserId(user.getUserId());

    chime.logoutUser(logoutUserRequest);
}
```

ユーザーの個人 PIN の更新

次の例は、指定した Amazon Chime ユーザーの個人会議 PIN をリセットする方法を示しています。

```
ResetPersonalPINRequest request = new ResetPersonalPINRequest()
    .withAccountId("chimeAccountId")
    .withUserId("userId");

ResetPersonalPINResult result = chime.resetPersonalPIN(request);

User user = result.getUser();
user.getPersonalPIN()
```

Amazon Chime デスクトップクライアントへのチャットボットの統合

AWS Command Line Interface (AWS CLI)、Amazon Chime API、または AWS SDK を使用して、チャットボットを Amazon Chime と統合できます。チャットボットを使用すると、Amazon Lex、AWS Lambda、および他の AWS のサービスの機能を使用して、 Amazon Chime チャットルーム内のユーザーがアクセスできるインテリジェントな会話型インターフェイスの一般的なタスクを合理化できます。

Amazon Chime エンタープライズアカウント管理者の場合は、ユーザーが次のようなタスクを実行できるようにするためにチャットボットを使用できます。

- 内部システムの情報をクエリする。
- タスクを自動化する。
- 重要な問題に関する通知を受信する。

- サポートチケットを作成する。

Amazon Chime エンタープライズアカウントの詳細については、「Amazon Chime アカウントの管理」を参照してください。

Amazon Chime エンタープライズアカウントを管理する場合、最大 10 個までのチャットボットを Amazon Chime と統合するために作成できます。チャットボットは、アカウントのメンバーが作成するチャットルーム内でのみ使用できます。チャットルーム管理者のみがチャットルームにチャットボットを追加できます。チャットルームにチャットボットが追加されると、チャットルームのメンバーはボットの作成者から提供されるコマンドを使用してこのボットとやり取りすることができます。詳細については、このトピックの次のセクションを参照してください。

Linux と macOS のユーザーは、サンプルのカスタムチャットボットを作成できます。詳細については、「Build custom chatbots for Amazon Chime」を参照してください。

コンテンツ

Amazon Chime を使用したチャットボットの使用

Amazon Chime エンタープライズアカウントを管理する場合、最大 10 個までのチャットボットを Amazon Chime と統合するために作成できます。チャットボットは、アカウントのメンバーが作成するチャットルーム内でのみ使用できます。チャットルーム管理者のみがチャットルームにチャットボットを追加できます。チャットルームにチャットボットが追加されると、チャットルームのメンバーはボットの作成者から提供されるコマンドを使用してこのボットとやり取りすることができます。詳細については、「Amazon Chime ユーザーガイド」の「Using chatbots」を参照してください。

また、Amazon Chime アカウントでチャットボットを有効または停止するために、Amazon Chime API オペレーションを使用することもできます。詳細については、「チャットボットの更新」を参照してください。

> **Note**
>
> チャットボットは削除できません。アカウントでチャットボットが使用されないようにするには、「Amazon Chime API リファレンス」の Amazon Chime UpdateBot API オペレーションを使用してください。チャットボットを停止すると、チャットルーム管理者はこれを

チャットルームから削除できますが、この管理者がチャットボットをチャットルームに追加することはできません。チャットルーム内で停止されたチャットボットを @言及するユーザーは、エラーメッセージを受信します。

前提条件

Amazon Chime とチャットボットを統合する手順を開始する前に、以下の前提条件を満たす必要があります。

- チャットボットを作成します。
- ボットにイベントを送信する発信エンドポイントを Amazon Chime に作成します。AWS Lambda 関数 ARN あるいは HTTPS エンドポイントから選択します。Lambda の詳細については、「AWS Lambdaデベロッパーガイド」を参照してください。

HTTPS エンドポイントの DNS ベストプラクティス

HTTPS エンドポイントに DNS を割り当てるとき、ベストプラクティスとして以下が推奨されます。

- ボットのエンドポイントに専用の DNS サブドメインを使用します。
- ボットのエンドポイントを示す A レコードのみを使用します。
- ドメインのハイジャックを防ぐために、DNS サーバーと DNS レジストラを保護します。
- ボットのエンドポイントに専用のパブリックに有効な TLS 中間証明書を使用します。
- ボットメッセージを操作する前に、ボットメッセージの署名を暗号で検証します。

チャットボットを作成したら、AWS Command Line Interface (AWS CLI) または Amazon Chime API オペレーションを使用して、次のセクションで説明するタスクを完了します。

タスク

- ステップ 1: チャットボットを Amazon Chime と統合する
- ステップ 2: Amazon Chime チャットボットのアウトバウンドエンドポイントを設定する
- ステップ 3: チャットボットを Amazon Chime チャットルームに追加する
- チャットボットリクエストの認証
- チャットボットの更新

ステップ 1: チャットボットを Amazon Chime と統合する

前提条件を満たしたら、AWS CLI または Amazon Chime API を使用してチャットボットを Amazon Chime と統合します。

> **Note**
>
> 次の手順で、チャットボットの名前と E メールアドレスを作成します。チャットボット名と E メールアドレスは、作成後に変更できません。

AWS CLI

AWS CLI を使用してチャットボットを統合するには

1. チャットボットを Amazon Chime と統合するには、AWS CLI で create-bot コマンドを使用します。

```
aws chime create-bot --account-id 12a3456b-7c89-012d-3456-78901e23fg45 --display-
name exampleBot --domain example.com
```

   a. 最大で 55 英数字または特殊文字 (+、-、% など) のチャットボット表示名を入力します。

   b. Amazon Chime エンタープライズアカウントの登録ドメイン名を入力します。

2. Amazon Chime から、ボット ID が含まれるレスポンスが返されます。

```
"Bot": {
        "CreatedTimestamp": "timeStamp",
        "DisplayName": "exampleBot",
        "Disabled": exampleBotFlag,
        "UserId": "1ab2345c-67de-8901-f23g-45h678901j2k",
        "BotId": "botId",
        "UpdatedTimestamp": "timeStamp",
        "BotType": "ChatBot",
        "SecurityToken": "securityToken",
        "BotEmail": "displayName-chimebot@example.com"
         }
```

3. ボット ID とボット E メールアドレスをコピーして保存し、次の手順で使用します。

Amazon Chime API

Amazon Chime API を使用してチャットボットを統合するには

1. チャットボットを Amazon Chime と統合するには、「Amazon Chime API リファレンス」の CreateBot API オペレーションを使用します。
   a. 最大で 55 英数字または特殊文字 (+、-、% など) のチャットボット表示名を入力します。
   b. Amazon Chime エンタープライズアカウントの登録ドメイン名を入力します。
2. Amazon Chime から、ボット ID が含まれるレスポンスが返されます。ボット ID と E メールアドレスをコピーして保存します。ボットのメールアドレスは次のようになります:*exampleBot*-chimebot@*example.com*

AWS SDK for Java

次のサンプルコードは、AWS SDK for Java を使用してチャットボットを統合する方法を示しています。

```
CreateBotRequest createBotRequest = new CreateBotRequest()
    .withAccountId("chimeAccountId")
    .withDisplayName("exampleBot")
    .withDomain("example.com");

chime.createBot(createBotRequest);
```

Amazon Chime から、ボット ID が含まれるレスポンスが返されます。ボット ID と E メールアドレスをコピーして保存します。ボットのメールアドレスは次のようになります:*exampleBot*-chimebot@*example.com*

ステップ 2: Amazon Chime チャットボットのアウトバウンドエンドポイントを設定する

Amazon Chime エンタープライズアカウントのチャットボット ID を作成したら、Amazon Chime がボットにメッセージを送信するために使用するアウトバウンドエンドポイントを設定します。アウトバウンドエンドポイントは、AWS Lambda 関数 ARN でも、前提条件の一部として作成した HTTPS エンドポイントでもかまいません。Lambda の詳細については、「AWS Lambda デベロッパーガイド」を参照してください。

> **Note**
>
> チャットボットのアウトバウンド HTTPS エンドポイントが設定されていない、または空の場合、チャットルーム管理者はチャットルームにチャットボットを追加できません。また、チャットルームのユーザーはこのボットとやり取りできません。

AWS CLI

チャットボットのアウトバウンドエンドポイントを設定するには、AWS CLI で put-events-configuration コマンドを使用します。Lambda 関数 ARN またはアウトバウンド HTTPS エンドポイントを設定します。

Lambda ARN

```
aws chime put-events-configuration --account-id 12a3456b-7c89-012d-3456-78901e23fg45
 --bot-id botId --lambda-function-arn arn:aws:lambda:us-
east-1:111122223333:function:function-name
```

HTTPS endpoint

```
aws chime put-events-configuration --account-id 12a3456b-7c89-012d-3456-78901e23fg45
 --bot-id botId --outbound-events-https-endpoint https://example.com:8000
```

Amazon Chime はボット ID と HTTPS エンドポイントで応答します。

```
{
    "EventsConfiguration": {
        "BotId": "BotId",
        "OutboundEventsHTTPSEndpoint": "https://example.com:8000"
    }
}
```

Amazon Chime API

チャットボットのアウトバウンドエンドポイントを設定するには、「Amazon Chime API リファレンス」の Amazon Chime PutEventsConfiguration API オペレーションを使用します。Lambda 関数 ARN またはアウトバウンド HTTPS エンドポイントを設定します。

- Lambda 関数 ARN を設定する場合 — Amazon Chime は Lambda を呼び出し、提供された Lambda 関数 ARN を呼び出すことを Amazon Chime 管理者の AWS アカウントに許可するアクセス権限を追加します。これには、Amazon Chime にこの関数を呼び出すアクセス許可があることを検証するリハーサル呼び出しが続きます。アクセス許可の追加が失敗した、またはリハーサル呼び出しが失敗した場合、`PutEventsConfiguration` リクエストは HTTP 4xx エラーを介します。
- アウトバウンド HTTPS エンドポイントを設定する場合 — Amazon Chime は、Challenge JSON ペイロードを使用した HTTP ポストリクエストを前のステップで提供した発信 HTTPS エンドポイントに送信して、エンドポイントを検証します。発信 HTTPS エンドポイントは、JSON 形式の Challenge パラメータにエコーバックすることで応答します。以下の例では、リクエストと有効な応答を示しています。

  Request

```
HTTPS POST

JSON Payload:
{
   "Challenge":"00000000000000000000",
   "EventType" : "HTTPSEndpointVerification"
}
```

  Response

```
HTTP/1.1 200 OK
Content-type: application/json

{
    "Challenge":"00000000000000000000"
}
```

  チャレンジハンドシェイクが失敗すると、`PutEventsConfiguration` リクエストは HTTPS 4xx エラーを返します。

AWS SDK for Java

次のサンプルコードは、AWS SDK for Java を使用してエンドポイントを設定する方法を示しています。

```
PutEventsConfigurationRequest putEventsConfigurationRequest = new
 PutEventsConfigurationRequest()
     .withAccountId("chimeAccountId")
     .withBotId("botId")
     .withOutboundEventsHTTPSEndpoint("https://www.example.com")
     .withLambdaFunctionArn("arn:aws:lambda:region:account-id:function:function-name");

 chime.putEventsConfiguration(putEventsConfigurationRequest):
```

ステップ 3: チャットボットを Amazon Chime チャットルームに追加する

チャットルーム管理者のみがチャットルームにチャットボットを追加できます。管理者は、ステップ 1 で作成したチャットボットの E メールアドレスを使用します。

チャットルームに Chatbot を追加するには

1. Amazon Chime デスクトップクライアントあるいはウェブアプリケーションを開きます。
2. 右上の歯車アイコンを選択してから、[ウェブフックとボットの管理] を選択します。
3. [Add bot] を選択します。
4. [E メールアドレス] に、使用するボットの E メールアドレスを入力します。
5. [Add] (追加) を選択します。

ボット名がチャットルーム一覧に表示されます。チャットボットをチャットルームに追加するために必要なアクションが他にもある場合は、そのアクションをチャットルーム管理者に伝えてください。

チャットボットがチャットルームに追加されたら、チャットボットのコマンドをチャットルームのユーザーに提供します。これを行う 1 つの方法は、チャットルーム招待を受け取ったときに、チャットルームにセカンドコマンドヘルプを送信するようにチャットボットをプログラムすることです。また、チャットボットユーザーが使用するヘルプコマンドを作成することも推奨されます。

チャットボットリクエストの認証

Amazon Chime チャットルームからチャットボットに送信されたリクエストを認証できます。これを行うには、リクエストに基づいて署名を計算します。次に、計算された署名がリクエストのヘッ

ダーの 1 つに一致することを検証します。Amazon Chime は HMAC SHA256 ハッシュを使用してこの署名を生成します。

チャットボットがアウトバウンド HTTPS エンドポイントを使用して Amazon Chime 用に設定されている場合、次の認証ステップを使用します。

アウトバウンド HTTPS エンドポイントが設定されているチャットボットへの Amazon Chime からの署名リクエストを検証するには

1. HTTP リクエストから [Chime-Signature] を取得します。
2. リクエストの [Chime-Request-Timestamp] ヘッダーおよび [body] を取得します。次に、2 つの要素の間を区切るために縦線を使用して文字列を形成します。
3. CreateBot 応答から [Security Token (セキュリティトークン)] を [HMAC_SHA_256] の最初のキーとして使用し、ステップ 2 で作成した文字列をハッシュします。
4. ハッシュされたバイトを Base64 エンコードで署名文字列にエンコーディングします。
5. この計算された署名と [Chime-Signature] ヘッダーの 1 つを比較します。

次のコードサンプルでは、Java を使用して署名を生成する方法を示しています。

```
       private final String DELIMITER = "|";
       private final String HMAC_SHA_256 = "HmacSHA256";

       private String generateSignature(String securityToken, String requestTime,
String requestBody)
       {
           try {
               final Mac mac = Mac.getInstance(HMAC_SHA_256);
               SecretKeySpec key = new SecretKeySpec(securityToken.getBytes(UTF_8),
HMAC_SHA_256);
               mac.init(key);
               String data = requestTime + DELIMITER + requestBody;
               byte[] rawHmac = mac.doFinal(data.getBytes(UTF_8));

               return Base64.getEncoder().encodeToString(rawHmac);
               }
           catch (Exception e) {
               throw e;
               }
        }
```

アウトバウンド HTTPS エンドポイントは、2 秒以内に `200 OK` を使用して Amazon Chime リクエストに応答する必要があります。それ以外の場合、このリクエストは失敗します。2 秒後にアウトバウンド HTTPS エンドポイントが使用不可である場合 (接続または読み取りタイムアウトのため)、あるいは Amazon Chime が 5xx 応答コードを受信する場合、Amazon Chime はリクエストを 2 回再試行します。1 回目の再試行は、最初のリクエストが失敗してから 200 ミリ秒後に送信されます。2 回目の再試行は、前の再試行が失敗してから 400 ミリ秒後に送信されます。2 回目の再試行後でも発信 HTTPS エンドポイントがまだ使用不可である場合、このリクエストは失敗します。

> **Note**
>
> [Chime-Request-Timestamp] はリクエストの再試行ごとに変更します。

Lambda 関数 ARN を使用して Amazon Chime 用のチャットボットが設定されている場合、次の認証ステップを使用します。

Lambda 関数 ARN が設定されているチャットボットへの Amazon Chime からの署名リクエストを検証するには

1. Lambda リクエスト ClientContext から Chime-Signature と Chime-Request-Timestamp を Base64 でエンコードされた JSON 形式で取得します。

   ```
   {
   "Chime-Signature" : "1234567890",
   "Chime-Request-Timestamp" : "2019-04-04T21:30:43.181Z"
   }
   ```

2. リクエストペイロードから [body] を取得します。
3. `CreateBot` 応答から [セキュリティトークン] を [HMAC_SHA_256] の最初のキーとして使用し、作成した文字列をハッシュします。
4. ハッシュされたバイトを Base64 エンコードで署名文字列にエンコーディングします。
5. この計算された署名と [Chime-Signature] ヘッダーの 1 つを比較します。

Lambda 呼び出し中に `com.amazonaws.SdkClientException` が発生する場合、Amazon Chime はリクエストを 2 回再試行します。

チャットボットの更新

Amazon Chime アカウント管理者は、Amazon Chime API と AWS SDK または AWS CLI を使用して、チャットボットの詳細を表示できます。アカウントでのチャットボットの使用を有効化または停止することもできます。また、チャットボットにセキュリティトークンを再生成することもできます。

詳細については、「Amazon Chime API リファレンス」の次のトピックを参照してください。

- GetBot – チャットボットの詳細を取得します (ボット E メールアドレスやボットタイプなど)。
- UpdateBot – アカウント内でチャットボットの使用を有効あるいは停止します。
- RegenerateSecurityToken – チャットボットにセキュリティトークンを再生成します。

また、チャットボットの `PutEventsConfiguration` を変更することもできます。例えば、チャットボットが当初発信 HTTPS エンドポイントを使用するように設定されている場合、前の設定イベントを削除して、Lambda 関数 ARN 用に新しいイベント設定を構築できます。

詳細については、「Amazon Chime API リファレンス」の次のトピックを参照してください。

- DeleteEventsConfiguration
- PutEventsConfiguration

チャットボットに送信される Amazon Chime イベント

次のイベントが Amazon Chime からチャットボットに送信されます。

- 招待 – チャットボットが Amazon Chime チャットルームに追加されたときに送信されます。
- 言及 – チャットルーム内のユーザーがチャットボットを @言及するときに送信されます。
- 削除 – Amazon Chime チャットルームからチャットボットが削除されたときに送信されます。

次の例では、これらのイベントごとにチャットボットに送信される JSON ペイロードを示しています。

Example : 招待イベント

```
            {
              "Sender": {
                           "SenderId": "user@example.com",
                           "SenderIdType": "EmailId"
                         },
              "Discussion": {
                           "DiscussionId": "abcdef12-g34h-56i7-j8kl-mn9opqr012st",
                           "DiscussionType": "Room"
                           },
              "EventType": "Invite",
              "InboundHttpsEndpoint": {
                                        "EndpointType": "Persistent",
                                        "Url": "https://
hooks.a.chime.aws/incomingwebhooks/a1b2c34d-5678-90e1-f23g-h45i67j8901k?
token=ABCDefGHiJK1LMnoP2Q3RST4uvwxYZAbC56DeFghIJkLM7N8OP9QRsTuV0WXYZABcdefgHiJ"
                                      },
              "EventTimestamp": "2019-04-04T21:27:52.736Z"
            }
```

Example : 言及イベント

```
            {
                "Sender": {
                           "SenderId": "user@example.com",
                           "SenderIdType": "EmailId"
                         },
                "Discussion": {
                               "DiscussionId": "abcdef12-g34h-56i7-j8kl-mn9opqr012st",
                               "DiscussionType": "Room"
                             },
                "EventType": "Mention",
                "InboundHttpsEndpoint": {
                                           "EndpointType": "ShortLived",
                                           "Url": "https://
hooks.a.chime.aws/incomingwebhooks/a1b2c34d-5678-90e1-f23g-h45i67j8901k?
token=ABCDefGHiJK1LMnoP2Q3RST4uvwxYZAbC56DeFghIJkLM7N8OP9QRsTuV0WXYZABcdefgHiJ"
                                         },
                "EventTimestamp": "2019-04-04T21:30:43.181Z",
                "Message": "@botDisplayName@example.com Hello Chatbot"
            }
```

> **Note**
>
> 言及イベントの InboundHttpsEndpoint URL は、送信後 2 分で有効期限が切れます。

Example : 削除イベント

```
{
    "Sender": {
                "SenderId": "user@example.com",
                "SenderIdType": "EmailId"
              },
    "Discussion": {
                    "DiscussionId": "abcdef12-g34h-56i7-j8kl-mn9opqr012st",
                    "DiscussionType": "Room"
                  },
    "EventType": "Remove",
    "EventTimestamp": "2019-04-04T21:27:29.626Z"
}
```

Amazon Chime 用のウェブフックの作成

ウェブフックを使用すると、ウェブアプリケーションはリアルタイムで相互に通信できます。通常、ウェブフックはアクションが発生すると通知を送信します。例えば、オンラインショッピングサイトを運営しているとします。ウェブフックは、顧客がショッピングカートに商品を追加したり、注文の支払いをしたり、コメントを送信したりしたときに通知を送信できます。ウェブフックは従来のアプリケーションほどプログラミングを必要とせず、処理能力もそれほど消費しません。ウェブフックを使用しない場合、プログラムはデータをリアルタイムで取得するために頻繁にデータをポーリングする必要があります。ウェブフックを使用する場合は、送信側アプリケーションがデータを即座に送信します。

着信ウェブフックは、プログラムによって Amazon Chime チャットルームにメッセージを送信できます。例えば、ウェブフックは新しい高優先度チケットの作成についてカスタマーサービスチームに通知を送信し、チケットへのリンクをチャットルームに追加できます。

ウェブフックメッセージは、マークダウンを使用してフォーマットすることができます。また、絵文字を含めることもできます。HTTP リンクや E メールアドレスは、アクティブなリンクとしてレンダリングされます。メッセージに @All や @Present と注釈を入れ、チャットルームのすべ

てのメンバーや現在のメンバーにそれぞれアラートを出すこともできます。チャットルーム参加者を直接 @mention するには、エイリアスまたは完全な電子メールアドレスを使用します。たとえば、@alias や @alias@domain.com などです。

ウェブフックはチャットルームの一部であり、共有することはできません。Amazon Chime のチャットルーム管理者は、チャットルームに最大 10 個のウェブフックを追加することができます。

ウェブフックを作成したら、次に示す手順に従って Amazon Chime チャットルームと統合できます。

ウェブフックとチャットルームを統合するには

1. チャットルーム管理者からウェブフック URL を入手します。詳細については、「Amazon Chime ユーザーガイド」の「Adding webhooks to a chat room」を参照してください。
2. 作成したスクリプトまたはアプリケーションのウェブフック URL を使用して、チャットルームにメッセージを送信します。

   a. この URL を使用して、HTTP POST リクエストを受け取ります。

   b. 単一キーの [コンテンツ] を含む JSON ペイロードが Amazon Chime ウェブフックに送信されます。以下は、サンプルペイロードを含むサンプル curl コマンドです。

```
curl -X POST "<Insert your webhook URL here>" -H "Content-Type:application/
json" --data '{"Content":"Message Body emoji test: :) :+1: link test: http://
sample.com email test: marymajor@example.com All member callout: @All All
 Present member callout: @Present"}'
```

   次に、Windows ユーザー向けの PowerShell コマンドの例を示します。

```
Invoke-WebRequest -Uri '<Insert your webhook URL here>' -Method 'Post' -
ContentType 'application/JSON' -Body '{"Content":"Message Body emoji test: :) :
+1: link test: http://sample.com email test: marymajor@example.com All member
 callout: @All All Present member callout: @Present"}'
```

外部プログラムより webhook URL に HTTP POST が送信されると、webhook が有効であることと、チャットルームが割り当てられていることがサーバーで検証されます。Webhook は、横に名前がついた Webhook アイコンでチャットルームの詳細に表示されます。Webhook によって送信されたチャットルームメッセージは、チャットルームで Webhook 名の下に表示され、その後に (Webhook) が続きます。

> **Note**
>
> CORS は現在、ウェブフックに対して有効になっていません。

ウェブフックに関連するエラーのトラブルシューティング

webhook 関連のエラーの一覧を以下に示します。

- webhook ごとの Incoming Webhook のレート制限は、1 TPS です。スロットリングの場合は、HTTP 429 エラーが返ります。
- webhook で投稿されるメッセージは、4 KB 以下である必要があります。メッセージのペイロードサイズがこのサイズを超えると、HTTP 413 エラーが返ります。
- @All や @Present と注釈を入れた webhook で投稿されたメッセージは、メンバーが 50 人以下のチャットルームに対してのみ有効です。メンバーが 50 人を超える場合、HTTP 400 エラーが返ります。
- webhook URL が再生成されている場合は、古い URL を使用すると、HTTP 404 エラーが返ります。
- ルームの webhook が削除されている場合は、古い URL を使用すると、HTTP 404 エラーが返ります。
- webhook URL が無効な場合は、HTTP 403 エラーが返ります。
- サービスが利用できない場合は、レスポンスとして HTTP 503 エラーが送信されます。

Amazon Chime の管理サポート

> **Note**
>
> Amazon ショッピングアカウントに関するヘルプは、amazon.com のカスタマーサービスにお問い合わせください。

Amazon Chime のサポートに問い合わせる必要がある場合は、以下のいずれかのオプションを選択してください。

- AWS Support アカウントをお持ちの場合は、Support センターにアクセスしてチケットを送信してください。
- お持ちでない場合、AWS Management Console を開き、[Amazon Chime]、[Support (サポート)、[Submit request] (リクエストの送信) の順に選択します。

以下の情報をできるだけ多く提供してください。

- 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。
- ご使用の Amazon Chime バージョン。バージョン番号を確認するには:
  - Windows で [Help] (ヘルプ)、[About Amazon Chime (Amazon Chime のバージョン情報) の順に選択します。
  - macOS で、[Amazon Chime]、[About Amazon Chime] (Amazon Chime の詳細) を選択します。
  - iOS および Android では、[設定]、[詳細] の順に選択します。
- ログ参照 ID。この ID を見つけるには:
  - Windows および macOS では、[ヘルプ]、[Send Diagnostic Logs] (診断ログの送信) を選択します。
  - iOS および Android では、[設定]、[Send Diagnostic Logs] を選択します。
- 問題が会議に関連している場合は、会議 ID です。

Amazon Chime 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。 AWS のお客様は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャ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 また、 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 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対象範囲内の AWS のサービス」を参照してください。
- クラウドのセキュリティ — 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 使用時に責任共有モデルが適用されるしくみを理解するうえで役立ちます。以下のトピックでは、セキュリティとコンプライアンスの目的を満たすように Amazon Chime を設定する方法について説明します。また、Amazon Chime リソースのモニタリングや保護に役立つ他の AWS 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 の Identity and Access Management
- Amazon Chime で IAM が機能するしくみ
- サービス間の混乱した代理の防止
- Amazon Chime リソースベースのポリシー
- Amazon Chime タグに基づいた認可
- Amazon Chime IAM ロール
- Amazon Chime のアイデンティティベースポリシーの例
- Amazon Chime 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 のサービスリンクロールの使用

- Amazon Chime での口グ記録とモニタリング
- Amazon Chime のコンプライアンス検証
- Amazon Chime の耐障害性
- Amazon Chime のインフラストラクチャセキュリティ
- Amazon Chime の自動更新について理解する

Amazon Chime 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 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 で行う作業によって異なります。

サービスユーザー - 業務を行うために Amazon Chime サービスを使用する場合は、管理者から必要な認証情報と許可が提供されます。業務のために使用する Amazon Chime 機能が増えるにつれて、追加の許可が必要になる可能性があります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。Amazon Chime の機能にアクセスできない場合は、「Amazon Chime アイデンティティとアクセスのトラブルシューティング」を参照してください。

サービス管理者 - 社内の Amazon Chime リソースを担当している場合は、Amazon Chime に対する完全なアクセス権があると思われます。サービスのユーザーがどの Amazon Chime 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。会社で Amazon Chime と IAM を併用する方法の詳細については、「Amazon Chime で IAM が機能するしくみ」を参照してください。

IAM 管理者 - IAM 管理者には、Amazon Chime へのアクセスを管理するポリシーの作成方法の詳細を理解することが推奨されます。IAM で使用できる Amazon Chime 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、Amazon Chime のアイデンティティベースポリシーの例 を参照してください。

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、フェデレーティッド 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、フェデレーティッド ID の例です。フェデレーティッド 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、多要素認証 (MFA) を使用してアカウントのセキュリティを向上させ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 およびリソースへの AWS のサービス 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、 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 – フェデレーティッド 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。フェデレーティッド 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 では 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 へのリクエストリクエスト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 に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービス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、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 のオブジェクトです。 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) AWS 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 に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は 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、フェデレーティッドユーザー、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 IAM の AWS マネージドポリシーを使用することはできません。

AWS Amazon Chime の マネージドポリシー

ユーザー、グループ、ロールにアクセス許可を追加するには、自分でポリシーを作成するよりも、AWS 管理ポリシーを使用する方が簡単です。チームに必要な権限のみを提供する IAM カスタマーマネージドポリシーを作成するには、時間と専門知識が必要です。すぐに開始するには、 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範囲に含めており、 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、 ReadOnlyアクセス 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。あるサービスで新しい機能を立ち上げる場合は、 AWS は、追加された演算とリソースに対し、読み込み専用の権限を追加します。ジョブ機能ポリシーのリストと説明については、IAM ユーザーガイドの「AWS ジョブ機能のマネージドポリシー」を参照してください。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための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もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

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 で IAM が機能するしくみ

IAM を使用して Amazon Chime へのアクセスを管理する前に、Amazon Chime で使用できる IAM 機能について理解しておく必要があります。Amazon Chime 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「IAM AWS 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 アイデンティティベースのポリシー
- リソース
- 例

Amazon Chime 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 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許可を付与するポリシーで使用されます。

条件キー

Amazon Chime は、サービス固有の条件キーを提供しません。すべての AWS グローバル条件キーを確認するには、IAM ユーザーガイドの「AWS グローバル条件コンテキストキー」を参照してください。

リソース

Amazon Chime では、ポリシーでリソースの Amazon ARN を指定することはできません。

例

Amazon Chime でのアイデンティティベースのポリシーの例は、「Amazon Chime のアイデンティティベースポリシーの例」でご確認ください。

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、リソースのセキュリティを保護するために、 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 が他のサービスに付与するそのリソースへの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 リソースベースのポリシー

Amazon Chime では、 リソースベースのポリシーはサポートされていません。

Amazon Chime タグに基づいた認可

Amazon Chime は、リソースのタグ付けやタグに基づいたアクセスの制御をサポートしていません。

Amazon Chime IAM ロール

IAM ロールは、特定のアクセス許可を持つ AWS アカウント内のエンティティです。

Amazon Chime 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GetFederationトークン などの AWS STS API オペレーションを呼び出します。

Amazon Chime は、一時的な認証情報の使用をサポートします。

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完了する他の 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 は、サービスリンクロールをサポートしています。Amazon Chime サービスリンクロールの作成または管理の詳細については、「Amazon Chime のサービスリンクロールの使用」を参照してください。

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、そうするとサービスの機能が損なわれる場合があります。

Amazon Chime は、サービスロールをサポートしていません。

Amazon Chime のアイデンティティベースポリシーの例

デフォルトでは、IAM ユーザーおよびロールにはAmazon Chime 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
- Amazon Chime コンソールの使用
- Amazon Chime へのフルアクセスをユーザーに許可する
- 自分の権限の表示をユーザーに許可する
- ユーザーにユーザー管理アクションへのアクセスを許可する
- AWS マネージドポリシー: AmazonChimeVoiceConnectorServiceLinkedRolePolicy
- 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

ID ベースのポリシーは、アカウント内で誰が Amazon Chime リソースを作成、アクセス、または削除できるかを決定します。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 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポ

リシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「AWS ジョブ機能の管理ポリシー」を参照してください。

- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、 などの特定の を介してサービスアクションが使用される場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素: 条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer ポリシーの検証」を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA 保護 API アクセスの設定」を参照してください。

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

Amazon Chime コンソールの使用

Amazon Chime コンソールにアクセスするには、許可の最小限のセットが必要です。これらのアクセス許可により、 AWS アカウント内の Amazon Chime リソースの詳細を一覧表示および表示できます。最小限必要な許可よりも厳しく制限されたアイデンティティベースポリシーを作成すると、そのポリシーを添付したエンティティ (IAM ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

これらのエンティティが引き続き Amazon Chime コンソールを使用できるようにするには、エンティティに次の AWS 管理AmazonChimeReadOnlyポリシーもアタッチします。詳細については、IAM ユーザーガイド」の「ユーザーへの許可の追加」を参照してください。

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

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

Amazon Chime へのフルアクセスをユーザーに許可する

次の AWS マネージドAmazonChimeFullAccessポリシーは、IAM ユーザーに Amazon Chime リソースへのフルアクセスを付与します。このポリシーは、ユーザーに対して、すべての Amazon Chime オペレーションへのアクセス、さらにユーザーに代わって Amazon Chime が実行できる必要のあるその他のオペレーションへのアクセスを許可します。

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

```
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketVersioning",
                "s3:GetBucketWebsite"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:GetLogDelivery",
                "logs:ListLogDeliveries",
                "logs:DescribeResourcePolicies",
                "logs:PutResourcePolicy",
                "logs:CreateLogGroup",
                "logs:DescribeLogGroups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes"
            ],
            "Resource": [
                "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sqs:GetQueueAttributes",
                "sqs:CreateQueue"
            ],
            "Resource": [
                "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
            ]
```

```
        }
    ]
}
```

自分の権限の表示をユーザーに許可する

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

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

```
}
```

ユーザーにユーザー管理アクションへのアクセスを許可する

AWS 管理AmazonChimeUserManagementポリシーを使用して、Amazon Chime コンソールのユーザー管理アクションへのアクセス権をユーザーに付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "chime:ListAccounts",
                "chime:GetAccount",
                "chime:GetAccountSettings",
                "chime:UpdateAccountSettings",
                "chime:ListUsers",
                "chime:GetUser",
                "chime:GetUserByEmail",
                "chime:InviteUsers",
                "chime:InviteUsersFromProvider",
                "chime:SuspendUsers",
                "chime:ActivateUsers",
                "chime:UpdateUserLicenses",
                "chime:ResetPersonalPIN",
                "chime:LogoutUser",
                "chime:ListDomains",
                "chime:GetDomain",
                "chime:ListDirectories",
                "chime:ListGroups",
                "chime:SubmitSupportRequest",
                "chime:ListDelegates",
                "chime:ListAccountUsageReportData",
                "chime:GetMeetingDetail",
                "chime:ListMeetingEvents",
                "chime:ListMeetingsReportData",
                "chime:GetUserActivityReportData",
                "chime:UpdateUser",
                "chime:BatchUpdateUser",
                "chime:BatchSuspendUser",
                "chime:BatchUnsuspendUser",
                "chime:AssociatePhoneNumberWithUser",
                "chime:DisassociatePhoneNumberFromUser",
```

```
                "chime:GetPhoneNumber",
                "chime:ListPhoneNumbers",
                "chime:GetUserSettings",
                "chime:UpdateUserSettings",
                "chime:CreateUser",
                "chime:AssociateSigninDelegateGroupsWithAccount",
                "chime:DisassociateSigninDelegateGroupsFromAccount"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS マネージドポリシー: AmazonChimeVoiceConnectorServiceLinkedRolePolicy

AmazonChimeVoiceConnectorServiceLinkedRolePolicy により、Amazon Chime Voice Connector は Amazon Kinesis Video Streams にメディアをストリーミングしたり、ストリーミング通知を提供したり、Amazon Polly を使用して音声を合成したりできます。このポリシーは、お客様の Amazon Kinesis Video Streams にアクセスしたり、Amazon Simple 通知サービスと Amazon Simple キューサービスに通知イベントを送信したり、Amazon Chime SDK 音声アプリケーションの Speak および SpeakAndGetDigits アクションを使用する際に Amazon Polly を使用して音声を合成したりする権限を Amazon Chime Voice Connector サービスに付与します。詳細については、「Amazon Chime SDK 管理者ガイド」の「Amazon Chime SDK identity-based policy examples」を参照してください。

AWS マネージドポリシーに対する Amazon Chime の更新

次の表に示すのは、Amazon Chime IAM ポリシーに関する更新の一覧と説明です。

変更	説明	日付
AmazonChimeVoiceConnectorServiceLinkedRolePolicy - 既存ポリシーへの更新	Amazon Chime Voice Connector に、Amazon Polly を使用して音声を合成できる新しい権限が追加されました。これらの権限は、Amazon Chime SDK 音声アプ	2022 年 3 月 15 日

変更	説明	日付
	リケーションの Speak および SpeakAndGetDigits アクションを使用する際に必要です。	
AmazonChimeVoiceConnectorServiceLinkedRolePolicy – 既存ポリシーへの更新	Amazon Chime Voice Connector に、Amazon Kinesis Video Streams へのアクセスを許可し、通知イベントを SNS と SQS に送信するための新しい権限が追加されました。Amazon Chime Voice Connector がメディアを Amazon Kinesis Video Streams にストリーミングし、ストリーミング通知を提供するには、これらの権限が必要です。	2021 年 12 月 20 日
既存のポリシー関する変更。Amazon Chime SDK ポリシーを使用した IAM ユーザーまたはロールの作成。	拡張検証をサポートする新しいアクションが Amazon Chime に追加されました。 出席者と会議リソースの一覧表示とタグ付けが可能になり、会議の文字起こしを開始および停止するためのアクションが追加されました。	2021 年 9 月 23 日
Amazon Chime が変更の追跡を開始	Amazon Chime 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 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

以下の情報を使用して、Amazon Chime 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てます。

トピック

Amazon Chime 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 を実行する権限がありません。PassRole

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Amazon Chime にロールを渡せるようにする必要があります。

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

以下の例では、marymajor という IAM ユーザーがコンソールを使用して Amazon Chime でアクションを実行しようする場合にエラーが発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、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 のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

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

AWS アカウント外のユーザーに Amazon Chime リソースへのアクセスを許可したい

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

詳細については、以下を参照してください:

- Amazon Chime がこれらの機能をサポートしているかどうかを確認するには、「Amazon Chime で IAM が機能するしくみ」を参照してください。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの外部認証されたユーザーへのアクセスの提供 (ID フェデレーション) を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いについては、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。

Amazon Chime のサービスリンクロールの使用

Amazon Chime は、AWS Identity and Access Management (IAM) サービスリンクロールを使用しています。サービスリンクロールは、Amazon Chime に直接リンクされた特殊なタイプの IAM ロールです。サービスリンクロールは Amazon Chime によって事前に定義されており、サービスがユーザーに代わって AWS のその他サービスを呼び出すために必要なすべての許可が含まれています。

サービスリンクロールでは、必要なアクセス許可を手動で追加する必要がないので、Amazon Chime を効率的に設定できます。サービスリンクロールの許可は Amazon Chime が定義し、別段の定義がない限り、Amazon Chime 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。

サービスにリンクされたロールは、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 リソースを保護します。

サービスにリンクされたロールをサポートす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。サービスにリンクされたロール列が「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

- Alexa for Business の共有デバイスでのロールの使用
- 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

Alexa for Business の共有デバイスでのロールの使用

以下のセクションでは、サービスリンクロールを使用し、Amazon Chime に AWS アカウント内の Alexa for Business リソースへのアクセス権を付与する方法について説明します。

トピック

- Amazon Chime のサービスリンクロールアクセス許可
- Amazon Chime のサービスリンクロールの作成
- Amazon Chime のサービスリンクロールの編集
- Amazon Chime 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 のサービスリンクロールアクセス許可

Amazon Chime で AWSServiceRoleForAmazonChime というサービスリンクロールを使用 – Alexa for Business共有 デバイスなど、Amazon Chime が使用または管理する AWS サービスおよびリソースへのアクセスを許可します。

AWSServiceRoleForAmazonChime サービスリンクロールは、以下のサービスを信頼してロールを引き受けます。

- `chime.amazonaws.com`

ロールアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを Amazon Chime に許可します。

- アクション: `arn:aws:iam::*:role/aws-service-role/chime.amazonaws.com/AWSServiceRoleForAmazonChime` 上で `iam:CreateServiceLinkedRole`

サービスリンクロールの作成、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 ユーザーガイドの「サービスリンクロールのアクセス許可」を参照してください。

Amazon Chime のサービスリンクロールの作成

サービスにリンクされたロールを手動で作成する必要はありません。AWS Management Console、AWS CLI、または AWS API で Amazon Chime の共有デバイスについて Alexa for Business をオンにすると、Amazon Chime がサービスリンクロールを作成します。

IAM コンソールを使用して、Amazon Chime ユースケースで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、`chime.amazonaws.com` サービス名を使用してサービスリンク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「サービスリンクロールの作成」を参照してください。このサービスリンクロールを削除する場合、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 のサービスリンクロールの編集

Amazon Chime では、AWSServiceRoleForAmazonChime サービスロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能

性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの編集」を参照してください。

Amazon Chime 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、使用していないエンティティがアクティブにモニターリングされたり、メンテナンスされたりすることがなくなります。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスリンクロールのクリーンアップ

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

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

AWSServiceRoleForAmazonChime (コンソール) が使用している Amazon Chime リソースを削除するには

- Amazon Chime アカウント内のすべての共有デバイスで Alexa for Business をオフにします。
  a. https://chime.aws.amazon.com/ で Amazon Chime コンソールを開きます。
  b. [Users (ユーザー)]、[Shared devices (共有デバイス)] を選択します。
  c. デバイスを選択します。
  d. [Actions] を選択します。
  e. [Disable Alexa for Business] (Alexa for Business を無効にする) を選択します。

サービスリンクロールを手動で削除する

IAM コンソール、AWS CLI、または AWS API を使用して、AWSServiceRoleForAmazonChime 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 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リンク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 ライブトランスクリプショ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。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 ライブトランスクリプションのサービスリンクロールアクセス許可
- Amazon Chime 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 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 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 ライブトランスクリプションのサービスリンクロールアクセス許可

Amazon Chime ライブトランスクリプションで AWSServiceRoleForAmazonChimeTranscription というサービスリンクロールを使用 — Amazon Chime がユーザーに代わって Amazon Transcribe および Amazon Transcribe Medical にアクセスできるようになります。

AWSServiceRoleForAmazonChimeTranscription サービスリンクロールは、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`

ロールアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを Amazon Chime に許可します。

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

サービスリンクロールの作成、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 ユーザーガイド」の「サービスにリンクされたロールの許可」を参照してください。

Amazon Chime 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. https://console.aws.amazon.com/iam/ で AWS マネジメントコンソールにサインインして、IAM コンソールを開きます。
2. IAM コンソールのナビゲーションペインで [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 トランスクリプション] を選択します。
4. [Next] (次へ) をクリックします。
5. [Next] (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 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。このサービスリンクロールを削除する場合、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 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 では、AWSServiceRoleForAmazonChimeTranscription サービス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 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

サービスにリンクされた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。

IAM を使用してサービスリンクロールを手動で削除するには

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「サービスにリンクされたロールの削除」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 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リンク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 で AWSServiceRoleForAmazonChimeSDKMediaPipelines というサービスリンクロールを使用 — 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。

AWSServiceRoleForAmazonChimeSDKMediaPipelines のサービスリンクロールは、以下のサービスを信頼してロールを引き受けます。

- `mediapipelines.chime.amazonaws.com`

このロールは、指定したリソースに対して以下のアクションを実行することを Amazon Chime に許可します。

- 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: `chime:GetMeeting` 上で `all AWS resources`

サービスリンクロールの作成、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 ユーザーガイド」の「サービスにリンクされたロールの許可」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 メディアパイプライン*ユースケースでサービスリンク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. https://console.aws.amazon.com/iam/ で AWS マネジメントコンソールにサインインして、IAM コンソールを開きます。

2. IAM コンソールのナビゲーションペインで [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. [Next] (次へ) をクリックします。
5. [Next] (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 mediapipelines.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。

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

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

Amazon Chime SDK パイプラインのサービスリンクロールの編集

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

Amazon Chime SDK 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。

IAM を使用してサービスリンクロールを手動で削除するには

IAM コンソール、AWS CLI、または AWS API を使用して、AWSServiceRoleForAmazonChimeSDKMediaPipelines サービスリンクロールを削除します。詳細については、「IAM ユーザーガイド」の「サービス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 メディアパイプラインのサービスリンクロールがサポートされるリージョン

Amazon Chime SDK は、このサービスを利用できるすべての AWS リージョンでサービスリンク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。

Amazon Chime でのログ記録とモニタリング

モニタリングは、Amazon Chime およびその他の AWS ソリューションの信頼性、可用性、およびパフォーマンスを維持する上で重要な部分です。AWS には、Amazon Chime リソースをモニタリングしたり、レポートを発行したり、必要に応じて自動アクションを実行したりするために以下のツールが用意されています。

- Amazon CloudWatch は、AWS リソースおよび AWS で実行しているアプリケーションをリアルタイムでモニタリングします。メトリクスの収集と追跡、カスタマイズしたダッシュボードの作成、および指定したメトリクス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の設定を行うことができます。例えば、CloudWatch で Amazon EC2 インスタンスの CPU 使用率などのメトリクスを追跡し、必要に応じて新しいインスタンスを自動的に起動できます。詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。
- Amazon EventBridge は、AWS リソースの変更を記述したシステムイベントのストリームをほぼリアルタイムに配信します。EventBridge は、自動化されたイベント駆動型のコンピューティングを可能にします。これにより、特定のイベントをモニタリングし、これらのイベントが発生したときに他の AWS サービスで自動アクションをトリガーするルールを記述できます。詳細については、「Amazon EventBridge ユーザーガイド」を参照してください。
- Amazon CloudWatch Logs は、Amazon EC2 インスタンス、CloudTrail、およびその他のソースからのログファイルをモニタリング、保存、およびアクセスするのに役立ちます。CloudWatch Logs は、ログファイル内の情報をモニタリングし、特定のしきい値が満たされたときに通知します。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可能です。詳細については、Amazon CloudWatch Logs ユーザーガイドを参照してください。
- AWS CloudTrail は、AWS アカウントによって呼び出されたか、またはそのアカウントに代わって呼び出された API コールとそれに関連するイベントを記録します。次に、指定した Amazon S3 バケットにログファイルが渡されます。AWS を呼び出したユーザーとアカウント、呼び出し元の IP アドレス、および呼び出しの発生日時を特定できます。詳細については、AWS CloudTrailユーザーガイドを参照してください。

トピック

Amazon CloudWatch による Amazon Chime のモニタリング

Amazon CloudWatch を使用して Amazon Chime をモニタリングすることで、raw データを収集し、ほぼリアルタイムに処理して読み取り可能なメトリクスできます。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やサービスの動作をより的確に把握できます。また、特定のしきい値をモニタリングするアラームを設定し、これらの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 CloudWatch ユーザーガイド」を参照してください。

Amazon Chime 用の CloudWatch メトリクス

Amazon Chime は、次のメトリクスを CloudWatch に送信します。

`AWS/ChimeVoiceConnector` 名前空間には、AWS アカウントおよび Amazon Chime Voice Connectors 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。

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。 単位はカウント

メトリクス	説明
OutboundCallAttempts	試行された発信通話の数。 単位はカウント
OutboundCallFailures	発信通話の失敗回数。 単位はカウント
OutboundCallsAnswered	応答された発信通話の数。 単位はカウント
OutboundCallsActive	現在アクティブな発信通話の数。 単位はカウント
Throttles	通話の試行時にアカウントがスロットルされる回数。 単位はカウント
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。 単位はカウント
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。 単位はカウント
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。 単位はカウント
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。 単位はカウント

メトリクス	説明
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。 単位はカウント
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。 単位はカウント
CustomerToVcRtpPackets	カスタマーから Amazon Chime 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。 単位はカウント
CustomerToVcRtpBytes	カスタマーから RTP パケットで Amazon Chime Voice Connector インフラストラクチャに送信されたバイト数。 単位はカウント
CustomerToVcRtcpPackets	カスタマーから Amazon Chime 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。 単位はカウント
CustomerToVcRtcpBytes	カスタマーから RTCP パケットで Amazon Chime Voice Connector インフラストラクチャに送信されたバイト数。 単位はカウント

メトリクス	説明
CustomerToVcPacketsLost	カスタマーから Amazon Chime 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。 単位はカウント
CustomerToVcJitter	カスタマーから Amazon Chime Voice Connector インフラストラクチャに送信されたパケットの平均ジッター。 単位: マイクロ秒
VcToCustomerRtpPackets	Amazon Chime Voice Connector インフラストラクチャからカスタマーに送信された RTP パケットの数。 単位はカウント
VcToCustomerRtpBytes	Amazon Chime Voice Connector インフラストラクチャから RTP パケットでカスタマーに送信されたバイト数。 単位はカウント
VcToCustomerRtcpPackets	Amazon Chime Voice Connector インフラストラクチャからカスタマーに送信された RTCP パケットの数。 単位はカウント
VcToCustomerRtcpBytes	Amazon Chime Voice Connector インフラストラクチャから RTCP パケットでカスタマーに送信されたバイト数。 単位はカウント

メトリクス	説明
VcToCustomerPacketsLost	Amazon Chime Voice Connector インフラストラクチャからカスタマーへの転送中に失われたパケットの数。 単位はカウント
VcToCustomerJitter	Amazon Chime Voice Connector インフラストラクチャからカスタマーに送信されたパケットの平均ジッター。 単位: マイクロ秒
RTTBetweenVcAndCustomer	カスタマーと Amazon Chime Voice Connector インフラストラクチャ間の平均往復時間。 単位: マイクロ秒
MOSBetweenVcAndCustomer	カスタマーと Amazon Chime Voice Connector インフラストラクチャの間を流れる音声ストリームに関連する推定平均オピニオンスコア (MOS)。 単位: 1.0 ~ 4.4 のスコア。スコアが高いほど、認識されるオーディオ品質が向上します。
RemoteToVcRtpPackets	リモートエンドから Amazon Chime 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。 単位はカウント
RemoteToVcRtpBytes	リモートエンドから RTP パケットで Amazon Chime Voice Connector インフラストラクチャに送信されたバイト数。 単位はカウント

メトリクス	説明
RemoteToVcRtcpPackets	リモートエンドから Amazon Chime 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。 単位はカウント
RemoteToVcRtcpBytes	リモートエンドから RTCP パケットで Amazon Chime Voice Connector インフラストラクチャに送信されたバイト数。 単位はカウント
RemoteToVcPacketsLost	リモートエンドから Amazon Chime 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。 単位はカウント
RemoteToVcJitter	リモートエンドから Amazon Chime Voice Connector インフラストラクチャに送信されたパケットの平均ジッター。 単位: マイクロ秒
VcToRemoteRtpPackets	Amazon Chime Voice Connector インフラストラクチャからリモートエンドに送信された RTP パケットの数。 単位はカウント
VcToRemoteRtpBytes	Amazon Chime Voice Connectors インフラストラクチャから RTP パケットでリモートエンドに送信されたバイト数。 単位はカウント

メトリクス	説明
VcToRemoteRtcpPackets	Amazon Chime Voice Connector インフラストラクチャからリモートエンドに送信された RTCP パケットの数。 単位はカウント
VcToRemoteRtcpBytes	Amazon Chime Voice Connectors インフラストラクチャから RTCP パケットでリモートエンドに送信されたバイト数。 単位はカウント
VcToRemotePacketsLost	Amazon Chime 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。 単位はカウント
VcToRemoteJitter	Amazon Chime Voice Connector インフラストラクチャからリモートエンドに送信されたパケットの平均ジッター。 単位: マイクロ秒
RTTBetweenVcAndRemote	リモートエンドと Amazon Chime Voice Connectors 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 Voice Connector インフラストラクチャの間を流れる音声ストリームに関連する推定平均オピニオンスコア (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。

Amazon Chime 用の CloudWatch ディメンション

Amazon Chime で使用できる CloudWatch ディメンションは以下のとおりです。

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

Amazon Chime 用の CloudWatch Logs

Amazon Chime Voice Connector メトリクスを CloudWatch Logs に送信できます。詳細については、「Amazon Chime SDK 管理ガイド」の「Editing Amazon Chime Voice Connector settings」を参照してください。

メディア品質メトリクスログ

Amazon Chime Voice Connectors にはメディア品質メトリクスログを受信するオプションが用意されています。これを選択すると、Amazon Chime は、作成された CloudWatch Logs ロググループについて、すべての Amazon Chime Voice Connector 通話に関する分単位の詳細なメトリクスを送信します。ロググループ名は /aws/ChimeVoiceConnectorLogs/${*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	通話を実行する Amazon Chime Voice Connector ID。
event_timestamp	メトリクスが出力された時刻 (ミリ秒単位)。UNIX エポック (1970 年 1 月 1 日の午前 0 時) からの経過時間 (UTC) で表示されます。
call_id	トランザクション ID に対応します。
from_sip_user	呼び出しの開始ユーザー。
from_country	呼び出しの発信国。

フィールド	説明
to_sip_user	呼び出しの受信ユーザー。
to_country	呼び出しの受信国。
endpoint_id	呼び出しのもう一方のエンドポイントを示す不透明な識別子。CloudWatch Logs Insights と組み合わせて使用します。詳細については、Amazon CloudWatch Logs ユーザーガイドの「CloudWatch Logs Insights を使用したログデータの分析」を参照してください。
aws_region	呼び出しの AWS リージョン。
cust2vc_rtp_packets	カスタマーから Amazon Chime 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	カスタマーから RTP パケットで Amazon Chime 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	カスタマーから Amazon Chime 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	カスタマーから RTCP パケットで Amazon Chime Voice Connector インフラストラクチャに送信されたバイト数。
cust2vc_packets_lost	カスタマーから Amazon Chime 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。
cust2vc_jitter	カスタマーから Amazon Chime Voice Connector インフラストラクチャに送信されたパケットの平均ジッター。

フィールド	説明
vc2cust_rtp_packets	Amazon Chime Voice Connector インフラストラクチャからカスタマーに送信された RTP パケットの数。
vc2cust_rtp_bytes	Amazon Chime Voice Connector インフラストラクチャから RTP パケットでカスタマーに送信されたバイト数。
vc2cust_rtcp_packets	Amazon Chime Voice Connector インフラストラクチャからカスタマーに送信された RTCP パケットの数。
vc2cust_rtcp_bytes	Amazon Chime Voice Connector インフラストラクチャから RTCP パケットでカスタマーに送信されたバイト数。
vc2cust_packets_lost	Amazon Chime Voice Connector インフラストラクチャからカスタマーへの転送中に失われたパケットの数。
vc2cust_jitter	Amazon Chime Voice Connector インフラストラクチャからカスタマーに送信されたパケットの平均ジッター。
rtt_btwn_vc_and_cust	カスタマーと Amazon Chime Voice Connector インフラストラクチャ間の平均往復時間。
mos_btwn_vc_and_cust	カスタマーと Amazon Chime Voice Connector インフラストラクチャの間を流れる音声ストリームに関連する推定平均オピニオンスコア (MOS)。
rem2vc_rtp_packets	リモートエンドから Amazon Chime 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。

フィールド	説明
rem2vc_rtp_bytes	リモートエンドから RTP パケットで Amazon Chime 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 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 パケットで Amazon Chime 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 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。
rem2vc_jitter	リモートエンドから Amazon Chime Voice Connector インフラストラクチャに送信されたパケットの平均ジッター。
vc2rem_rtp_packets	Amazon Chime Voice Connector インフラストラクチャからリモートエンドに送信された RTP パケットの数。
vc2rem_rtp_bytes	Amazon Chime Voice Connectors インフラストラクチャから RTP パケットでリモートエンドに送信されたバイト数。
vc2rem_rtcp_packets	Amazon Chime 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 Voice Connectors インフラストラクチャから RTCP パケットでリモートエンドに送信されたバイト数。

フィールド	説明
vc2rem_packets_lost	Amazon Chime 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。
vc2rem_jitter	Amazon Chime Voice Connector インフラストラクチャからリモートエンドに送信されたパケットの平均ジッター。
rtt_btwn_vc_and_rem	リモートエンドと Amazon Chime Voice Connectors 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 Voice Connector インフラストラクチャの間を流れる音声ストリームに関連する推定平均オピニオンスコア (MOS)。

SIP メッセージログ

Amazon Chime Voice Connectors について SIP メッセージログの受信を選択できます。受け取りを選択すると、Amazon Chime により、インバウンドおよびアウトバウンドの SIP メッセージがキャプチャされ、作成された CloudWatch Logs ロググループにこのメッセージが送信されます。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 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 Voice Connector 通話 ID。

フィールド	説明
sip_message	キャプチャされた完全な SIP メッセージ。

EventBridge による Amazon Chime の自動化

Amazon EventBridge を使用すると、AWS サービスを自動化して、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 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 は生成したイベントをベストエフォートで配信で EventBridge に送信し、これは Amazon Chime がすべてのイベントを EventBridgeに送信しようとするけれどもまれにイベントが配信されないことがあることを意味します。詳細については、Amazon EventBridge ユーザーガイドの「AWS サービスからのイベント」を参照してください。

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

EventBridge による Amazon Chime Voice Connector の自動化

Amazon Chime Voice Connector について自動的にトリガーできる アクションには、以下があります。

- 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 で EventBridge を使用する例を以下に示します。

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

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

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

Amazon Chime Voice Connector は、このセクションで説明するイベントの発生時に EventBridge へのイベントの送信をサポートします。

Amazon Chime Voice Connector ストリーミング開始

Amazon Chime Voice Connector は、Kinesis Video Streams へのメディアストリーミング開始時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@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",
        "streamArn": "arn:aws:kinesisvideo:us-east-1:123456:stream/ChimeVoiceConnector-
abcdef1ghij2klmno3pqr4-111aaa-22bb-33cc-44dd-111222/111122223333",
        "toNumber": "+13605550199",
        "transactionId": "12345678-1234-1234",
        "voiceConnectorId": "abcdef1ghij2klmno3pqr4",
        "streamingStatus": "STARTED",
        "version": "0"
    }
}
```

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

Amazon Chime Voice Connector は、Kinesis Video Streams へのメディアストリーミング終了時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 Voice Connector ストリーミング更新

Amazon Chime Voice Connector は、Kinesis Video Streams へのメディアストリーミング更新時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",
```

```
        "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 Voice Connector ストリーミング失敗

Amazon Chime Voice Connector は、Kinesis Video Streams へのメディアストリーミング失敗時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 を使用した Amazon Chime API コールのログ記録

Amazon Chime は AWS CloudTrail と統合され、このサービスは Amazon Chime 内のユーザー、ロール、または AWS サービスによって実行されたアクションのレコードを提供します。CloudTrail は、Amazon Chime コンソールからの呼び出し、および API へのコード呼び出しを含む、Amazon Chime のすべての API コールをイベントとしてキャプチャします。証跡を作成する場合は、Amazon Chime のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。追跡を設定しない場合でも、CloudTrail コンソールの [Event history] (イベント履歴) で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、Amazon Chime に送られたリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

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

CloudTrail 内の Amazon Chime

AWS アカウントを作成すると、そのアカウントに対して CloudTrail が有効になります。Amazon Chime 管理コンソールから API コールが呼び出されると、そのアクティビティは CloudTrail イベントに記録され、他の AWS サービスのイベントとともに [Event history] (イベント履歴) に記録されます。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、「CloudTrail Event 履歴でのイベントの表示」を参照してください。

Amazon Chime のイベントなど、AWS アカウントのイベントの継続的な記録を残すには、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで追跡を作成するときに、追跡がすべての リージョンに適用されます。追跡は、AWSパーティションのすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、その他の AWS サービスを設定して、CloudTrail ログで収集したイベントデータをより詳細に分析し、それに基づく対応を行うことができます。詳細については、以下を参照してください。

- 証跡を作成するための概要
- CloudTrail がサポートされているサービスと統合
- CloudTrail の Amazon SNS 通知の設定

- 「CloudTrail ログファイルを複数のリージョンから受け取る」および「複数のアカウントから CloudTrail ログファイルを受け取る」

すべての Amazon Chime アクションは CloudTrail が記録し、これらのアクションについては Amazon Chime リファレンスで説明しています。例えば、`CreateAccount`、`InviteUsers`、および `ResetPersonalPIN` セクションを呼び出すと、 CloudTrail ログファイルにエントリが生成されます。各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。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、ロールとフェデレーティッドユーザーのどちらかの一時的なセキュリティ認証情報を使用して送信されたかどうか。
- リクエストが、別の AWS のサービスによって送信されたかどうか。

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

Amazon Chime ログファイルエントリの理解

「トレイル」は、指定した Simple Storage Service (Amazon S3) バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルには、単一か複数のログエントリがあります。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報が含まれます。CloudTrail ログファイルは、公開 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 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 アカウントに Active Directory を設定している場合、「CloudTrail を使用した AWS Directory Service API コール」を参照してください。これは、Amazon Chime ユーザーのサインイン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ています。

以下の例は、の Amazon Chime 用の CloudTrail ログエントリを示します。

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

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


Amazon Chime 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 — 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 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ーゾーンを中心に構築されています。 AWS リージョンは、低レイテンシー、高スループット、および高度に冗長なネットワークで接続された、物理的に分離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、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ーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

Amazon Chime は、 AWS グローバルインフラストラクチャに加えて、データの耐障害性とバックアップのニーズに対応できるようにさまざまな機能を提供しています。詳細については、「Amazon Chime SDK 管理ガイド」の「Managing Amazon Chime Voice Connector groups」および「Streaming Amazon Chime Voice Connector media to Kinesis」を参照してください。

Amazon Chime 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 Amazon Chime 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 が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、「 Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

が AWS 公開した 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。

Amazon Chime の自動更新について理解する

Amazon Chime には、クライアントを更新するさまざまな方法が用意されています。ユーザーが Amazon Chime をブラウザで起動するか、デスクトップで起動するか、モバイル端末で起動するかによって、方法が異なります。

Amazon Chime ウェブアプリケーション - https://app.chime.aws - 常に最新の機能とセキュリティ修正を含めてロードします。

Amazon Chime デスクトップクライアントは、ユーザーが [Quit (終了) または [Sign Out] (サインアウト) を選択するたびに更新の有無を確認します。これは、Windows と macOS のコンピュータに適用されます。実行されたクライアントは、3 時間ごとに更新の有無を確認します。ユーザーはまた、Windows のヘルプメニューまたは macOS の Amazon Chime メニューで [Check for Updates] (更新プログラムの確認) を選択しても更新の有無を確認できます。

デスクトップクライアントがアップデートを検出すると、会議中でない限り、Amazon Chime がインストールを促します。以下のユーザーは進行中の会議に参加していることになります。

- 会議に出席している。
- まだ進行中の会議に招待された。

Amazon Chime は、最新バージョンをインストールするように促し、15 秒間の秒読みを設け、インストールの延期を可能にします。アップデートを延期する場合は、[Try Later] を選択します。

更新を延期した場合、会議に出席していなければ、クライアントは 3 時間後に更新の有無を確認して、もう一度インストールを促します。秒読みが終了するとインストールが開始されます。

> **Note**
>
> macOS ユーザーは [Restart Now] (今すぐ再起動) を選択してアップデートを開始する必要があります。

モバイルデバイス上 - Amazon Chime モバイルアプリケーションは、App Store および Google Play が提供する更新オプションを使用して、Amazon Chime クライアントの最新バージョンを配信します。モバイルデバイス管理システムを通して更新を配布することもできます。このトピックでは、以下のことがわかっていること前提としています。

Amazon Chime のドキュメント履歴

以下の表は、Amazon Chime 管理者ガイドに関する 2018 年 3 月以降の重要な変更点をまとめたものです。このドキュメントの更新に関する通知を受け取るために、RSS フィードをサブスクライブすることができます。

変更	説明	日付
「Amazon Chime SDK 管理ガイド」の公開	Amazon Chime SDK のトピックが 「Amazon Chime SDK 管理ガイド」に公開されるようになりました。詳細については、「Amazon Chime SDK 管理ガイド」を参照してください。	2022 年 3 月 24 日
IAM ポリシーの更新	によって管理される IAM AWS ポリシーへの変更は、この管理者ガイドで追跡されるようになりました。「 Amazon Chime identity-based policy examples」を参照してください。	2021 年 9 月 23 日
サービスリンクロール	管理者は、Amazon Live Transcription のサービスリンクロールを作成し、Amazon Chime ライブトランスクリプションオペレーションの開始時と終了時にイベントメッセージを表示できるようになりました。詳細については、「ライブトランスクリプションでのロールの使用」および「イベントによる Amazon	2021 年 8 月 12 日

	Chime の自動化」を参照してください。 CloudWatch	
SIP メディアアプリケーションおよびルール	管理者は、Amazon Chime AWS Lambda 音声コネクタと機能で使用するための SIP メディアアプリケーションとルールを作成できます。詳細については、Amazon Chime 管理者ガイドの「SIP アプリケーションとルールの管理」を参照してください。	2020 年 11 月 18 日
Amazon Chime Voice Connector 緊急通報ルーティング番号	Amazon Chime では、Amazon Chime Voice Connector の緊急通報ルーティング番号を設定できます。詳細については、Amazon Chime 管理者ガイドの「Amazon Chime 音声コネクタの緊急通報ルーティング番号の設定」を参照してください。	2020 年 7 月 1 日
ドルビーボイス Huddle の Amazon Chime	Amazon Chime は、ドルビーボイス Huddle の音声およびビデオ会議ハードウェアで、ネイティブまたはファーストパーティの会議体験を提供します。詳細については、『Amazon Chime 管理者ガイド』の「ドルビーハードウェアでの Amazon Chime のセットアップ」を参照してください。	2020 年 6 月 3 日

チャット保持ポリシーの設定	Amazon Chime 管理者は、エンタープライズアカウントのチャット保持ポリシーを設定できます。詳細については、Amazon Chime 管理者ガイドの「チャット保持ポリシーの管理」を参照してください。	2020 年 5 月 21 日
チャットメッセージの削除	プログラミングができる場合は、Amazon Chime API のペアを使用して、アカウント内のチャットルームや会話からメッセージを削除できます。詳細については、Amazon Chime 管理者ガイドの「個々のメッセージの削除」を参照してください。	2020 年 5 月 18 日
CloudWatch Amazon Chime 音声コネクターのメディア品質メトリクス	Amazon Chime は、Amazon Chime 音声コネクタのメディア品質メトリックスをに送信することをサポートしています。 CloudWatch詳細については、『Amazon Chime 管理者ガイド』の「Amazon Chime CloudWatch によるモニタリング」を参照してください。	2020 年 1 月 23 日
Slack 用の Amazon Chime 会議アプリケーション	Amazon Chime は、Slack 用の Amazon Chime 会議アプリケーションに対応しています。詳細については、Amazon Chime 管理者ガイドの「Slack 用 Amazon Chime ミーティングアプリのセットアップ」を参照してください。	2019 年 12 月 4 日

会議リージョンの設定	Amazon Chime は、 AWS すべての参加者にとって最適なリージョンでの会議の処理をサポートします。詳細については、Amazon Chime 管理者ガイドの「ミーティングリージョンの設定」を参照してください。	2019 年 12 月 3 日
SIP-Based Media Recording (SIPREC) の互換性	Amazon Chime Voice Connector は、SIPREC 互換音声インフラストラクチャから Kinesis Video Streams へのメディアストリーミングをサポートしています。詳細については、Amazon Chime 管理者ガイドの「SIP ベースのメディアレコーディング (SIPREC) の互換性」を参照してください。	2019 年 11 月 25 日
ドルビーボイスルームの Amazon Chime	ドルビーボイスルームの音声およびビデオ会議ハードウェアで、ネイティブまたはファーストパーティの会議エクスペリエンスを提供する Amazon Chime を利用すれば、ユーザーが簡単に会議に参加できるようにすることができます。詳細については、『Amazon Chime 管理者ガイド』の「ドルビーボイスルームでの Amazon Chime のセットアップ」を参照してください。	2019 年 10 月 29 日

発信通話の発信者名の更新	Amazon Chime インベントリ内の電話番号を使用して発信される通話で受信者に表示されるデフォルトの発信者名を設定します。詳細については、Amazon Chime 管理者ガイドの「アウトバウンドコール名の更新」を参照してください。	2019 年 10 月 24 日
Amazon Kinesis へのメディアストリーミング	分析や機械学習などの処理のために Amazon Chime Voice Connector から Amazon Kinesis Video Streams に電話の音声をストリーミングします。詳細については、Amazon Chime 管理者ガイドの「Amazon Chime 音声コネクタメディアを Kinesis にストリーミングする」および「Amazon Chime 音声コネクタサービスにリンクされたロールを使用する」を参照してください。	2019 年 10 月 24 日
アマゾンによる Amazon Chime のモニタリング CloudWatch	Amazon Chime CloudWatch を使用してモニタリングします。Amazon Chime は未加工データを収集し、読み取り可能でほぼリアルタイムのメトリックスに処理します。詳細については、『Amazon Chime 管理者ガイド』の「Amazon Chime CloudWatch によるモニタリング」を参照してください。	2019 年 10 月 24 日

Amazon Chime Voice Connector グループ	AWS さまざまなリージョンで作成された Amazon Chime 音声コネクタを含む Amazon Chime 音声コネクタグループを作成します。これにより、受信通話がリージョン間でフェイルオーバーされ、可用性イベントが発生した場合にフォールバックするためのフォールトトレラントなメカニズムが作成されます。詳細については、Amazon Chime 管理者ガイドの「Amazon Chime 音声コネクタグループの使用」を参照してください。	2019 年 10 月 24 日
ネットワーク設定の更新	Amazon Chime は、ファイアウォールの要件を簡素化します。詳細については、Amazon Chime 管理者ガイドの「ネットワーク設定と帯域幅要件」を参照してください。	2019 年 9 月 6 日
モデレート会議	Amazon Chime はモデレート会議に対応しています。詳細については、Amazon Chime 管理者ガイドの「モデレート会議への参加」を参照してください。	2019年7月25日
Amazon Chime のコンプライアンス検証	Amazon Chime は HIPAA 対応サービスです。詳細については、Amazon Chime 管理者ガイドの「Amazon Chime のコンプライアンス検証」を参照してください。	2019 年 6 月 11 日

通話料無料の番号の移植	Amazon Chime は、Amazon Chime Voice Connector で使用する米国の通話料無料の番号の移植をサポートしています。詳細については、Amazon Chime 管理者ガイドの「既存の電話番号の移植」を参照してください。	2019 年 5 月 28 日
Amazon Chime での電話番号の管理	Amazon Chime Business Calling を使用して、電話番号をプロビジョニングして既存の Amazon Chime ユーザーに割り当てます。既存の電話システムにの Amazon Chime Voice Connector を統合します。詳細については、Amazon Chime 管理者ガイドの「Amazon Chime での電話番号の管理」を参照してください。	2019 年 3 月 18 日
Outlook 用 Amazon Chime アドイン	Amazon Chime は Outlook 用に 2 つのアドインを提供しています。Windows の Outlook 用 Amazon Chime アドインと Microsoft Outlook 用 Amazon Chime アドインです。これらのアドインは同じスケジュール機能を提供しますが、異なるタイプのユーザーをサポートします。詳細については、Amazon Chime 管理者ガイドの「Outlook 用アドインのデプロイ」を参照してください。	2019 年 3 月 12 日

さまざまな更新	トピックレイアウトと組織へのさまざまな更新。	2019 年 2 月 11 日
Amazon Chime コールミー機能	管理者は、[Meetings] (会議) の下で Amazon Chime コールミー機能を有効にできます。詳細については、Amazon Chime 管理者ガイドの「会議設定の管理」を参照してください。	2018 年 8 月 22 日
Okta SSO に接続	エンタープライズアカウントを持っている場合、Okta SSO に接続して認証し、ユーザーにアクセス許可を割り当てることができます。詳細については、『Amazon Chime 管理者ガイド』の「Okta SSO Connect する」を参照してください。	2018 年 8 月 1 日
ユーザーの添付ファイルをリクエストする	ユーザーによって Amazon Chime にアップロードされた添付ファイルを受信します。詳細については、Amazon Chime 管理者ガイドの「ユーザーアタッチメントのリクエスト」を参照してください。	2018 年 4 月 23 日
追加レポートデータの表示。	追加レポートデータの表示。詳細については、Amazon Chime 管理者ガイドの「レポートを表示する」を参照してください。	2018 年 3 月 30 日

ユーザーにプロまたはベーシックアクセス許可を割り当てます。	ユーザーにプロまたはベーシックアクセス許可を割り当てます。詳細については、Amazon Chime 管理者ガイドの「ユーザーアクセスとアクセス権限の管理」を参照してください。	2018 年 3 月 29 日