aws

ユーザーガイド

AWS エンドユーザーメッセージングソーシャル

AWS エンドユーザーメッセージングソーシャル: ユーザーガイド

Table of Contents

AWS エンドユーザーメッセージングソーシャルとは

AWS エンドユーザーメッセージングソーシャルは、ソーシャルメッセージングとも呼ばれ、デベロッパーがアプリケーション WhatsApp に統合できるようにするメッセージングサービスです。WhatsAppの豊富なメッセージング機能にアクセスできるため、イメージ、動画、ボタンを使用してブランド化されたインタラクティブなコンテンツを作成できます。このサービスを使用すると、SMS や プッシュ通知などの既存のチャネルとともにアプリケーションに WhatsApp メッセージング機能を追加できるため、希望する通信チャネルを通じて顧客とやり取りできます。

開始するには、 AWS エンドユーザーメッセージングソーシャルコンソールのセルフガイドオンボーディングプロセスを使用して新しい WhatsApp ビジネスアカウント (WABA) を作成するか、既存のWABAを サービスにリンクします。

トピック

初めての AWS エンドユーザーメッセージングソーシャルユーザーですか？

AWS エンドユーザーメッセージングソーシャルを初めて使用する場合は、まず以下のセクションを読むことをお勧めします。

- AWS エンドユーザーメッセージングソーシャルの設定
- AWS エンドユーザーメッセージングソーシャルの開始方法
- AWS エンドユーザーメッセージングソーシャルのベストプラクティス

AWS エンドユーザーメッセージングソーシャルの機能

AWS エンドユーザーメッセージングソーシャルには、次の機能と機能があります。

- メッセージテンプレートを作成して使用することで、一貫性のあるメッセージを設計し、コンテンツをより効果的に再利用します。メッセージテンプレートには、送信するメッセージで再利用するコンテンツと設定が含まれています。
- 新しいリッチメッセージング機能にアクセスして、より魅力的なエクスペリエンスを実現します。テキストやメディア以外にも、ロケーションやインタラクティブメッセージを送信できます。
- 顧客から受信するテキストおよびメディアメッセージを受信します。
- Meta を通じてビジネスアイデンティティを検証することで、顧客との信頼を構築します。

関連サービス

AWS は、マルチチャネルワークフローで一緒に使用できる他のメッセージングサービスを提供します。

- AWS エンドユーザーメッセージングSMSを使用してSMSメッセージを送信する
- AWS エンドユーザーメッセージングプッシュを使用してプッシュ通知を送信する
- Amazon SES を使用して E メールを送信する

AWS エンドユーザーメッセージングソーシャルへのアクセス

以下を使用して、 AWS エンドユーザーメッセージングソーシャルにアクセスできます。

AWS エンドユーザーメッセージングソーシャルコンソール

リソースを作成して管理するウェブインターフェイス。

AWS Command Line Interface

コマンドラインシェルのコマンドを使用して AWS サービスとやり取りします。 AWS Command Line Interface は、Windows、macOS 、および Linux でサポートされています。の詳細については AWS CLI、AWS Command Line Interface 「 ユーザーガイド」を参照してください。 AWS SMS コマンドは、 AWS CLI コマンドリファレンス にあります。

AWS SDKs

HTTP または 経由でリクエストを送信するAPIsのではなく、言語固有のアプリケーションの構築を希望するソフトウェアデベロッパーの場合HTTPS、 はライブラリ、サンプルコード、チュートリアル、その他のリソース AWS を提供します。これらのライブラリは、リクエストへの暗号化による署名、リクエストの再試行、エラーレスポンスの処理など、タスクを自動化する基本的

な機能を提供します。これらの関数は、開始をより効率的にするのに役立ちます。詳細については、「AWSでの構築ツール」を参照してください。

リージョナルな可用性

AWS エンドユーザーメッセージングソーシャルは、北米、欧州、アジア、オセアニア AWS リージョン の複数の で利用できます。各リージョンで、 は複数のアベイラビリティーゾーン AWS を維持します。これらのアベイラビリティーゾーンは物理的に相互に分離されていますが、低レイテンシーで高スループットの冗長性に優れたプライベートネットワーク接続で統合されています。これらのアベイラビリティーゾーンは、レイテンシーを最小限に抑えながら、非常に高いレベルの可用性と冗長性を提供するために使用されます。

の詳細については AWS リージョン、「 でAWS リージョン アカウントで使用できるものを指定する」を参照してくださいAmazon Web Services 全般のリファレンス。 AWS エンドユーザーメッセージングソーシャルが現在利用可能なすべてのリージョンと各リージョンのエンドポイントのリストについては、「」または以下の表の「エンドユーザーメッセージングソーシャルエンドポイントとサービスエンドポイントのエンドポイントとクォータ」を参照してください。 AWS API AWS Amazon Web Services 全般のリファレンス各リージョンで利用できるアベイラビリティーゾーンの数の詳細については、「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。

利用可能なリージョン

リージョン名	リージョン	エンドポイント	WhatsApp API バージョン
米国東部 (バージニア北部)	us-east-1	social-messaging.us-east-1.amazonaws.com social-messaging-fips.us-east-1.api.aws social-messaging.us-east-1.api.aws	バージョン 20 以降
米国東部 (オハイオ)	us-east-2	social-messaging.us-east-2.amazonaws.com	バージョン 20 以降

リージョン名	リージョン	エンドポイント	WhatsApp API バージョン
		social-messaging-fips.us-east-2.api.aws social-messaging.us-east-2.api.aws	
米国西部 (オレゴン)	us-west-2	social-messaging.us-west-2.amazonaws.com social-messaging-fips.us-west-2.api.aws social-messaging.us-west-2.api.aws	バージョン 20 以降
アジアパシフィック (ムンバイ)	ap-south-1	social-messaging.ap-south-1.amazonaws.com social-messaging.ap-south-1.api.aws	バージョン 20 以降
アジアパシフィック (シンガポール)	ap-southeast-1	social-messaging.ap-southeast-1.amazonaws.com social-messaging.ap-southeast-1.api.aws	バージョン 20 以降
欧州 (アイルランド)	eu-west-1	social-messaging.eu-west-1.amazonaws.com social-messaging.eu-west-1.api.aws	バージョン 20 以降

リージョン名	リージョン	エンドポイント	WhatsApp API バージョン
欧州 (ロンドン)	eu-west-2	social-messaging.eu-west-2.amazonaws.com social-messaging.eu-west-1.api.aws	バージョン 20 以降

AWS エンドユーザーメッセージングソーシャルの設定

AWS エンドユーザーメッセージングソーシャルを初めて使用する前に、次の手順を完了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

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/サインアップ 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 は、サインアッププロセスが完了した後に確認 E メールを送信します。https://aws.amazon.com/ に移動し、マイアカウント を選択すると、いつでも現在のアカウント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、 のセキュリティを確保し AWS アカウントのルートユーザー、 を有効にして管理ユーザーを作成し 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、「 ユーザーガイド」の AWS アカウント 「ルートユーザー (コンソール) の仮想MFAデバイスの有効化」を参照してください。 IAM

管理アクセスを持つユーザーを作成する

1. IAM Identity Center 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 Identity Center で、ユーザーに管理アクセスを許可します。

   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、 AWS IAM Identity Center ユーザーガイドの「デフォルトを使用してユーザーアクセスを設定する IAM アイデンティティセンターディレクトリ」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 Identity Center ユーザーでサインインするには、IAMIdentity Center ユーザーの作成時に E メールアドレスにURL送信されたサインインを使用します。

  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 Identity Center で、最小権限のアクセス許可を適用するベストプラクティスに従う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。

次のステップ

これで、 AWS エンドユーザーメッセージングソーシャルを使用する準備ができました。 WhatsApp ビジネスアカウントの作成 (WABA) または既存の WhatsApp ビジネスアカウントの移行AWS エンドユーザーメッセージングソーシャルの開始方法については、「」を参照してください。

AWS エンドユーザーメッセージングソーシャルの開始方法

これらのトピックでは、 WhatsApp ビジネスアカウント (WABA) を AWS エンドユーザーメッセージングソーシャルにリンクまたは移行する手順について説明します。

トピック

にサインアップする WhatsApp

WhatsApp ビジネスアカウント (WABA) を使用すると、ビジネス WhatsApp プラットフォームを使用して顧客にメッセージを直接送信できます。すべての WABAsは Meta ビジネスポートフォリオの一部です。WABA には、電話番号、テンプレート、 WhatsApp ビジネスプロファイルなどの顧客向けアセットが含まれます。 WhatsApp ビジネスプロファイルには、ユーザーが表示するビジネスの連絡先情報が含まれます。 WhatsApp ビジネスアカウントの詳細については、「」を参照してくださいWhatsApp AWS エンドユーザーメッセージングソーシャルのビジネスアカウント (WABA) 。

このセクションの手順に従って、 AWS エンドユーザーメッセージングソーシャルの使用を開始します。埋め込みサインアッププロセスを使用して、新しい WhatsApp ビジネスアカウント (WABA) を作成するか、既存の WABAを AWS エンドユーザーメッセージングソーシャルに移行します。

前提条件

Important

Meta/ の使用WhatsApp

- お客様による WhatsApp ビジネスソリューションの使用には、 WhatsApp サービス利用規約 、 WhatsApp ビジネスソリューション利用規約 、 WhatsApp ビジネスメッセージングポリシー 、 WhatsApp メッセージングガイドライン の利用規約、およびそれらに参照として組み込まれているその他のすべての条件、ポリシー、またはガイドライン (それぞれが随時更新される場合があります) が適用されます。
- Meta または WhatsApp は、いつでも WhatsApp ビジネスソリューションの使用を禁止することができます。
- Meta と で WhatsApp ビジネスアカウント (WABA「」) を作成する必要がありますWhatsApp。

- Meta で Business Manager アカウントを作成し、 にリンクする必要がありますWABA。
- お客様は、 のコントロールWABAを当社に提供する必要があります。お客様のリクエストに応じて、Meta が提供できる方法を使用して、合理的かつ適時にお客様のWABAバックコントロールをお客様に移管します。
- WhatsApp ビジネスソリューションの使用に関連して、お客様は、適用される法律や規制に従って、配布の保護や制限の対象となるコンテンツ、情報、またはデータを送信しません。
- WhatsApp WhatsApp ビジネスソリューションの使用に関する の料金は、「会話ベースの料金」に記載されています。

- WhatsApp ビジネスアカウント (WABA) を作成するには、ビジネスに Meta Business アカウントが必要です。会社がすでに Meta Business アカウントを持っているかどうかを確認します。Meta Business アカウントがない場合は、サインアッププロセス中に作成できます。
- メ WhatsApp ッセンジャーアプリケーションまたは WhatsApp ビジネスアプリケーションで既に使用されている電話番号を使用するには、まず電話番号を削除する必要があります。
- SMS または音声のワンタイムパスコード () を受信できる電話番号OTP。サインアップに使用される電話番号が WhatsApp アカウントに関連付けられ、メッセージを送信するときに電話番号が使用されます。電話番号はSMS、、MMS、および 音声メッセージングに引き続き使用できます。
- 既存の をインポートする場合はWABA、インポートされた に関連付けられているすべての電話番号PINsに が必要ですWABA。紛失または忘れた をリセットするにはPIN、 WhatsApp ビジネスプラットフォームクラウドAPIリファレンス の「更新PIN」の指示に従います。

コンソールからサインアップする

新しい WhatsApp アカウントの作成、既存のアカウントの移行、既存の への電話番号の追加を行うには、次の手順に従ってくださいWABA。サインアッププロセスの一環として、 WhatsApp ビジネスアカウントへの AWS エンドユーザーメッセージングソーシャルアクセスを許可します。また、AWS エンドユーザーメッセージングソーシャルがメッセージに対して請求することを許可します。WhatsApp ビジネスアカウントの詳細については、「」を参照してください WhatsApp ビジネスアカウントタイプについて。

1. で AWS エンドユーザーメッセージングソーシャルコンソールを開きますhttps://console.aws.amazon.com/social-messaging/。
2. ビジネスアカウント を選択します。

3. ビジネスアカウントのリンクページで、Facebook ポータルを起動 を選択します。Meta から新しいログインウィンドウが表示されます。
4. メタログインウィンドウで、Facebook アカウントの認証情報を入力します。

   WhatsApp ビジネスアカウントページで、電話番号の追加 WhatsApp を選択します。 WhatsApp 電話番号の追加ページで、Facebook ポータルの起動 を選択します。Meta から新しいログインウィンドウが表示されます。
5. メタログインウィンドウで、Facebook アカウントの認証情報を入力します。
6. サインアッププロセスの一環として、 WhatsApp ビジネスアカウント () への AWS エンドユーザーメッセージングソーシャルアクセスを許可しますWABA。また、 AWS エンドユーザーメッセージングソーシャルがメッセージに対して請求することを許可します。[Continue] (続行) を選択します。
7. Meta Business アカウント では、既存の Meta Business アカウント を選択するか、Meta Business アカウント を作成します。

   a. (オプション) Meta Business アカウントを作成する必要がある場合は、以下の手順に従います。
   b. ビジネス名 には、ビジネスの名前を入力します。
   c. ビジネスウェブサイトまたはプロファイルページ の場合は、会社のウェブサイトURLの を入力するか、会社のウェブサイトがない場合は、ソーシャルメディアページURLに を入力します。
   d. 国 の場合は、ビジネスが所在する国を選択します。
   e. (オプション) アドレスを追加を選択し、企業のアドレスを入力します。
8. [Next (次へ)] を選択します。
9. WhatsApp ビジネスアカウントを選択する では、既存の WhatsApp ビジネスアカウント (WABA) を選択するか、アカウントを作成する必要がある場合は、 WhatsApp ビジネスアカウントの作成 を選択します。

   WhatsApp ビジネスプロファイルを作成または選択するには、既存の WhatsApp ビジネスプロファイルを選択するか、新しい WhatsApp ビジネスプロファイルを作成します。
10. [Next (次へ)] を選択します。
11. ビジネスプロファイルを作成する には、次の情報を入力します。

    - WhatsApp ビジネスアカウント名 には、アカウントの名前を入力します。このフィールドは顧客向けではありません。

- WhatsApp ビジネスプロファイル表示名 には、お客様からメッセージを受け取ったときに表示する名前を入力します。表示名として会社名を使用することをお勧めします。名前は Meta によってレビューされ、WhatsApp表示名ルール に準拠する必要があります。会社名とは異なるブランド名を使用するには、会社とブランドの間に外部で公開された関連付けが必要です。この関連付けは、ウェブサイトおよび表示名のウェブサイトで表されるブランドに表示される必要があります。

  登録が完了すると、Meta は表示名の確認を実行します。Meta は、表示名が承認または拒否されたかどうかを知らせる E メールを送信します。表示名が拒否されると、1 日あたりのメッセージング制限が引き下げられ、 から切断される可能性があります WhatsApp。

  > **Important**
  >
  > 表示名を変更するには、Meta サポートを使用してチケットを作成する必要があります。

- タイムゾーン では、ビジネスが所在するタイムゾーンを選択します。
- カテゴリ では、ビジネスに最も適したカテゴリを選択します。お客様は、連絡先情報の一部としてカテゴリを表示できます。
- ビジネスの説明 には、会社の説明を入力します。お客様は、連絡先情報の一部としてビジネスの説明を表示できます。
- ウェブサイト には、会社のウェブサイトを入力します。お客様は、連絡先情報の一部としてウェブサイトを表示できます。
- [Next (次へ)] を選択します。

12. の電話番号を追加する WhatsAppには、登録する電話番号を入力します。この電話番号は、メッセージを送信するときに顧客に表示されます。
13. 番号の確認方法を選択するには、テキストメッセージまたは電話のいずれかを選択します。

    - 検証コードを受け取る準備ができたら、次へ を選択します。
    - 検証コードを入力し、次へ を選択します。

14. 番号が確認されたら、次へ を選択して Meta からウィンドウを閉じます。
15. WhatsApp ビジネスアカウントの場合、タグを展開します。オプションで、 WhatsApp ビジネスアカウントにタグを追加します。

    タグはキーと値のペアであり、必要に応じて AWS リソースに適用してアクセスや使用状況を制御できます。新しいタグを追加を選択し、アタッチするキーと値のペアを入力します。

16. WhatsApp ビジネスアカウントには、ビジネスアカウントと WhatsApp ビジネスアカウントに関連付けられたすべてのリソースのイベントをログに記録するためのメッセージとイベントの送信先を 1 つ持つことができます WhatsApp 。カスタマーメッセージの受信のログ記録など SNS、Amazon でイベントログ記録を有効にするには、メッセージとイベント発行 を有効にする必要があります。詳細については、「AWS エンドユーザーメッセージングソーシャルのメッセージとイベントの送信先」を参照してください。

    > **Important**
    >
    > カスタマーメッセージに応答できるようにするには、メッセージとイベント発行 を有効にする必要があります。

    メッセージとイベントの宛先の詳細セクションで、イベント発行 をオンにします。Amazon ではSNS、新しい Amazon SNS標準トピックを選択し、トピック名 に名前を入力するか、既存の Amazon SNS標準トピックを選択し、トピックの arn ドロップダウンリストからトピックを選択します。

17. 電話番号 の下：

    電話番号 の下にある各WhtsApp 電話番号について：

    a. 電話番号の検証 には、既存の を入力するPINか、新しいPINコードを入力します。紛失または忘れた をリセットするにはPIN、 WhatsApp ビジネスプラットフォームクラウドAPIリファレンス の「更新PIN」の指示に従います。

    b. 追加設定の場合：

        i. データローカリゼーションリージョン - オプションで、保管中のデータを保存する Meta のリージョンのいずれかを選択します。Meta のデータプライバシーポリシーの詳細については、 WhatsApp ビジネスプラットフォームクラウドAPIリファレンスの「データプライバシーとセキュリティ」と「クラウドAPIローカルストレージ」を参照してください。

        ii. タグはキーと値のペアであり、必要に応じて AWS リソースに適用してアクセスや使用状況を制御できます。新しいタグを追加を選択し、アタッチするキーと値のペアを入力します。

18. WhatsApp ビジネスアカウントには、ビジネスアカウントと WhatsApp ビジネスアカウントに関連付けられたすべてのリソースのイベントをログに記録するためのメッセージとイベントの送信先を 1 つ持つことができます WhatsApp 。カスタマーメッセージの受信のログ記録など

SNS、Amazon でイベントログ記録を有効にするには、メッセージとイベント発行 を有効にする必要があります。詳細については、「AWS エンドユーザーメッセージングソーシャルのメッセージとイベントの送信先」を参照してください。

> **Important**
>
> カスタマーメッセージに応答できるようにするには、メッセージとイベントの発行を有効にする必要があります。

メッセージとイベントの送信先の詳細セクションで、イベント発行 をオンにします。Amazon ではSNS、新しい Amazon SNS標準トピックを選択し、トピック名 に名前を入力するか、既存の Amazon SNS標準トピックを選択し、トピックの arn ドロップダウンリストからトピックを選択します。

19. セットアップを完了するには、電話番号の追加 を選択します。

次のステップ

サインアップが完了したら、メッセージの送信を開始できます。大規模なメッセージ送信を開始する準備ができたら、ビジネス検証 を完了します。 WhatsApp ビジネスアカウントと AWS エンドユーザーメッセージングソーシャルアカウントがリンクされたので、次のトピックを参照してください。

- イベントを口グに記録し、受信メッセージを受信するためのイベント送信先について説明します。
- メッセージテンプレート を作成する方法について説明します。
- テキストまたはメディアメッセージを送信する方法について説明します。
- メッセージを受信する方法について説明します。
- 公式ビジネスアカウントについて学び、表示名の横に緑色のチェックマークを付けて、メッセージのスループットを向上させます。

WhatsApp AWS エンドユーザーメッセージングソーシャルのビジネスアカウント (WABA)

WhatsApp ビジネスアカウント (WABA) を使用すると、ビジネス WhatsApp プラットフォームを使用して顧客にメッセージを直接送信できます。すべての WABAsは Meta Business Portfolio の一部です。 WhatsApp ビジネスアカウントには、電話番号、テンプレート、ビジネス連絡先情報などの顧客向けアセットが含まれます。は 1 つの にのみ存在WABAできます AWS リージョン。 WhatsApp ビジネスアカウントの詳細については、 WhatsAppビジネスプラットフォームクラウドリファレンスの「ビジネスアカウントWhatsApp API」を参照してください。

Important

Meta/ の使用WhatsApp

- お客様による WhatsApp ビジネスソリューションの使用には、 WhatsApp サービス利用規約 、 WhatsApp ビジネスソリューション利用規約 、 WhatsApp ビジネスメッセージングポリシー 、 WhatsApp メッセージングガイドライン の利用規約、およびそれらに参照として組み込まれているその他すべての条件、ポリシー、またはガイドライン (それぞれが随時更新される場合があります) が適用されます。
- Meta または WhatsApp は、いつでも WhatsApp ビジネスソリューションの使用を禁止することができます。
- Meta と を使用して WhatsApp ビジネスアカウント (WABA「」) を作成する必要がありますす WhatsApp。
- Meta を使用して Business Manager アカウントを作成し、 にリンクする必要がありますWABA。
- お客様は、 のコントロールWABAを当社に提供する必要があります。お客様のリクエストに応じて、Meta が提供できる方法を使用して、合理的かつ適時にお客様のWABAバックコントロールをお客様に移管します。
- WhatsApp ビジネスソリューションの使用に関連して、お客様は、適用される法律および/または規制に従って、配布の保護および/または制限の対象となるコンテンツ、情報、またはデータを送信しません。
- WhatsApp WhatsApp ビジネスソリューションの使用に関する の料金は、https://developers.facebook.com/docs/Whatsapp/pricing で確認できます。

トピック

- AWS エンドユーザーメッセージングソーシャルで WhatsApp ビジネスアカウント (WABA) を表示する
- AWS エンドユーザーメッセージングソーシャルに WhatsApp ビジネスアカウント (WABA) を追加する
- WhatsApp ビジネスアカウントタイプについて

AWS エンドユーザーメッセージングソーシャルで WhatsApp ビジネスアカウント (WABA) を表示する

WABA 関連付けられた を表示するには、以下の指示に従います AWS アカウント。

1. で AWS エンドユーザーメッセージングソーシャルコンソールを開きますhttps://console.aws.amazon.com/social-messaging/。
2. ビジネスアカウントでは、 を選択しますWABA。
3. 電話番号タブには、電話番号、表示名、品質評価、その日に残したビジネス開始の会話の数が表示されます。

   イベント送信先タブで、イベントの送信先を表示します。イベント送信先を編集するには、「」の指示に従いますAWS エンドユーザーメッセージングソーシャルのメッセージとイベントの送信先。

   テンプレートタブで、メッセージテンプレートの管理を選択して、Meta で WhatsApp テンプレートを編集します。各テンプレートの制限WABAは 250 です。

   タグタブでは、WABAリソースタグを管理できます。

AWS エンドユーザーメッセージングソーシャルに WhatsApp ビジネスアカウント (WABA) を追加する

WhatsApp ビジネスプロファイルを既にお持ちの場合は、アカウントに新しい WABAを追加します。新しい の作成の一環として、電話番号を に追加WABAする必要がありますWABA。

- アカウントに新しい を追加するには、WABA「」のステップに従いますAWS エンドユーザーメッセージングソーシャルの開始方法。

- ステップ 8 で、 WhatsApp ビジネスプロファイルを選択し、新しい WhatsApp ビジネスアカウントを作成する を選択します。

WhatsApp ビジネスアカウントタイプについて

WhatsApp ビジネスアカウントは、顧客にどのように表示されるかを決定します。 WhatsApp アカウントを作成すると、アカウントはビジネスアカウント になります。 には 2 種類のビジネスアカウント WhatsApp があります。

- ビジネスアカウント： WhatsApp ビジネスプラットフォーム上のすべてのアカウントの真正性 WhatsApp を検証します。ビジネスアカウントがビジネス検証プロセスを完了した場合、ビジネスの名前は、ユーザーがアドレス帳にビジネスを追加していない場合でも表示されます。この機能は、ユーザーが で検証済みのビジネスアカウントを識別するのに役立ちます WhatsApp。
- 公式ビジネスアカウント : ビジネスアカウントの利点に加えて、公式ビジネスアカウントには、プロファイルとチャットスレッドヘッダーに緑色のチェックマークバッジがあります。

  WhatsApp 公式ビジネスアカウント (OBA) の承認には、記事、ブログ投稿、独立レビューなどを通じて、ビジネスが有名であり、コンシューマーによって認識されていることを示す証拠を提供する必要があります。ビジネスが必要なドキュメントを提供している場合でも、 の承認 WhatsApp OBAは保証されません。承認プロセスは、 によるレビューと承認の対象となります WhatsApp。 は、公式ビジネスアカウントのアプリケーションの評価と承認に使用する特定の基準を公開 WhatsApp しません。を求める WhatsApp OBA企業は評判と評価を示す必要がありますが、最終的な承認は の裁量に委ねられます WhatsApp。

WhatsApp アカウントを作成すると、アカウントはビジネスアカウント になります。ウェブサイト、住所、時間など、ビジネスに関する情報を顧客に提供できます。 WhatsApp ビジネス検証を完了していないビジネスの場合、表示名は、チャットリストや個々のチャットではなく、連絡先ビューの電話番号の横にある小さなテキストでのみ表示されます。メタビジネス検証が完了すると、WhatsApp送信者の表示名がチャットリストと個々のチャットスレッドに表示されます。

追加リソース

- Business Account と Official Business Account の詳細については、Business Platform Cloud Reference の「Business Accounts」を参照してください。 WhatsApp API
- ビジネス検証プロセスの詳細については、 ビジネスプラットフォームクラウドリファレンス の「ビジネス検証WhatsApp API」を参照してください。

AWS エンドユーザーメッセージングソーシャルの電話番号

すべての WhatsApp ビジネスアカウントには、 との WhatsApp ID の検証に使用される 1 つ以上の電話番号が含まれており、送信 ID の一部として使用されます。 WhatsApp ビジネスアカウント (WABA) に複数の電話番号を関連付けて、異なるブランドの各電話番号を使用できます。

トピック

WhatsApp ビジネスアカウントで使用する電話番号に関する考慮事項

電話番号を WhatsApp ビジネスアカウント (WABA) にリンクする場合は、次の点を考慮する必要があります。

- 電話番号はWABA一度に 1 つにのみリンクできます。
- 電話番号はSMS、、MMS、および 音声通話に引き続き使用できます。
- 各電話番号は Meta の品質評価を受けています。

以下の操作SMSを行うことで、 AWS エンドユーザーメッセージングを通じて SMS対応電話番号を取得できます。

1. 電話番号の国またはリージョンが双方向 をサポートしていることを確認しますSMS。
2. 電話番号 をリクエストします。国または地域によっては、電話番号の登録が必要になる場合があります。
3. 電話番号の双方向SMSメッセージングを有効にします。セットアップが完了すると、受信SMSメッセージはイベント送信先に送信されます。

WhatsApp ビジネスアカウントに電話番号を追加する (WABA)

電話番号を既存の WhatsApp ビジネスアカウント (WABA) に追加するか、電話番号WABAの新しいを作成できます。

前提条件

開始する前に、次の前提条件を満たす必要があります。

- 電話番号は、 SMSまたは音声のワンタイムパスコード () を受信できる必要がありますOTP。これは、 に追加される電話番号ですWABA。
- 電話番号を他の に関連付けることはできませんWABA。

に電話番号を追加する WABA

既存の に新しい電話番号を追加するには WABA

1. で AWS エンドユーザーメッセージングソーシャルコンソールを開きますhttps://console.aws.amazon.com/social-messaging/。
2. ビジネスアカウント を選択し、電話番号 を追加します WhatsApp。
3. WhatsApp 電話番号の追加ページで、Facebook ポータルの起動 を選択します。Meta から新しいログインウィンドウが表示されます。
4. Meta ログインウィンドウで、Meta デベロッパーアカウントの認証情報を入力し、ビジネスポートフォリオを選択します。
5. 電話番号を追加する WABAと WhatsApp ビジネスプロファイルを選択します。
6. [Next (次へ)] を選択します。
7. の電話番号を追加する WhatsAppには、登録する電話番号を入力します。この電話番号は、メッセージを送信するときに顧客に表示されます。
8. 番号の確認方法を選択するには、テキストメッセージまたは電話のいずれかを選択します。
9. 検証コードを受け取る準備ができたら、次へを選択します。
10. 検証コードを入力し、次へ を選択します。番号が確認されたら、次へ を選択して Meta からウィンドウを閉じます。
11. WhtsApp 電話番号 の下：

a. 電話番号の検証 には、既存の を入力するPINか、新しいPINコードを入力します。紛失または忘れた をリセットするにはPIN、 WhatsApp ビジネスプラットフォームクラウドAPIリファレンス の「更新PIN」の指示に従います。

b. 追加設定の場合：

i. データローカリゼーションリージョン - オプションで、保管中のデータを保存する Meta のリージョンのいずれかを選択します。Meta のデータプライバシーポリシーの詳細については、 WhatsAppビジネスプラットフォームクラウドAPIリファレンスの「データプライバシーとセキュリティ」と「クラウドAPIローカルストレージ」を参照してください。

ii. タグはキーと値のペアであり、必要に応じて AWS リソースに適用してアクセスや使用状況を制御できます。新しいタグを追加を選択し、アタッチするキーと値のペアを入力します。

12. WhatsApp ビジネスアカウントには、ビジネスアカウントと WhatsApp ビジネスアカウントに関連付けられたすべてのリソースのイベントを口グに記録するためのメッセージとイベントの送信先を 1 つ持つことができます WhatsApp 。カスタマーメッセージの受信の口グ記録など SNS、Amazon でイベント口グ記録を有効にするには、メッセージとイベント発行 をオンにします。詳細については、「AWS エンドユーザーメッセージングソーシャルのメッセージとイベントの送信先」を参照してください。

> **Important**
>
> カスタマーメッセージに応答できるようにするには、メッセージとイベントの発行を有効にする必要があります。

メッセージとイベントの送信先の詳細セクションで、イベント発行 をオンにします。Amazon ではSNS、新しい Amazon SNS標準トピックを選択し、トピック名 に名前を入力するか、既存の Amazon SNS標準トピックを選択し、トピックの arn ドロップダウンリストからトピックを選択します。

13. セットアップを完了するには、電話番号の追加 を選択します。

電話番号のステータスを表示する

AWS End User Messaging Social でメッセージを送信できるようにするには、電話番号のステータスがアクティブである必要があります。

1. で AWS エンドユーザーメッセージングソーシャルコンソールを開きますhttps://console.aws.amazon.com/social-messaging/。
2. [電話番号] を選択します。
3. 電話番号セクションでは、ステータス列に各電話番号のステータスが表示されます。

> **Note**
>
> 電話番号のステータスが不完全なセットアップ の場合、電話番号を選択してからセットアップの完了を選択して電話番号の設定を完了します。

AWS エンドユーザーメッセージングソーシャルで電話番号の ID を表示する

を使用してメッセージを送信できるようにするには AWS CLI、送信時に使用する電話番号を識別する電話番号 ID が必要です。

1. で AWS エンドユーザーメッセージングソーシャルコンソールを開きますhttps://console.aws.amazon.com/social-messaging/。
2. [電話番号] を選択します。
3. 電話番号 セクションで、電話番号を選択します。
4. 電話番号の詳細セクションには、電話番号の電話番号 ID が含まれます。

でのメッセージング会話の制限を増やす WhatsApp

メッセージングの制限は、ビジネス電話番号が 24 時間以内に開くことができるビジネス主導の会話の最大数を指します。ビジネス電話番号は、当初、24 時間の移行期間に 250 件のビジネス主導の会話に制限されます。この制限は、メッセージの品質評価と送信するメッセージの数に基づいて、Meta によって引き上げることができます。ビジネス主導の会話では、テンプレートメッセージのみを使用できます。

カスタマーからメッセージを受け取ると、24 時間サービスウィンドウが開きます。この間、すべてのメッセージタイプ を送信できます。

以下のガイドラインに従うことで、メッセージの上限を 1,000 メッセージに引き上げることができます。

- 会社の電話番号はアクティブステータス である必要があります。
- ビジネス電話番号の品質評価が低い場合、品質評価が改善するまで、1 日あたり 250 件のビジネス主導の会話に制限される可能性があります。
- ビジネス検証 を申請します。ビジネスが承認されると、メッセージング品質が分析され、メッセージングアクティビティがメッセージング制限を引き上げる必要があるかどうかを判断します。分析に基づいて、メッセージング制限の引き上げのリクエストは Meta によって承認または拒否されます。
- ID 検証 を申請します。ID 検証を完了し、ID が確認された場合、Meta はメッセージング制限の引き上げを承認します。
- 質の高い評価のテンプレートを使用して、30 日間の引越し期間中に 1,000 回以上のビジネス主導の会話を開きます。会話のしきい値が 1,000 に達すると、メッセージング品質が分析され、メッセージングアクティビティがメッセージング制限を引き上げる必要があるかどうかを判断します。目標は、高品質のメッセージを一貫して送信し、メッセージングの制限を引き上げることです。

Business Verification または Identity Verification を完了した場合、または 1,000 件以上のビジネス会話を開いた場合でも、250 件のビジネス主導の会話に制限されている場合は、Meta にメッセージ階層のアップグレードをリクエストしてください。

ビジネスまたはアイデンティティの検証が拒否された場合、高品質のメッセージを送信することで、承認を受ける可能性を高めることができます。高品質、準拠、オプトインのメッセージを送信することで、メッセージングアクティビティと品質が再評価され、承認されたメッセージング機能が増加する可能性があります。

のメッセージング品質スコア WhatsApp は、最近のユーザーのフィードバックとインタラクションに基づいて計算され、より最近のデータにより多くの重みが与えられます。これにより、プラットフォームでのメッセージングの全体的な品質と信頼性を評価することができます。

メッセージ制限レベルの増加

- 1K ビジネス主導の会話
- 10K 件のビジネス主導の会話

- 100K 件のビジネス主導の会話
- ビジネス主導の会話の数に制限なし

でのメッセージスループットの向上 WhatsApp

メッセージスループットは、電話番号の 1 秒あたりの受信メッセージと送信メッセージの数 (MPS) です。デフォルトでは、各電話番号の は 80 MPSです。Meta は、以下の要件を満たすと、 を 1,000 MPSに増やすことができます。

- 電話番号は、ビジネス主導の会話を無制限に送信できる必要があります
- 電話番号の品質評価は中以上である必要があります。

での電話番号の品質評価について WhatsApp

電話番号とメッセージの品質は Meta によって決まります。メッセージング品質スコアは、過去 7 日間に顧客がメッセージを受信した方法に基づいており、最新のメッセージはより重みが付けられています。メッセージング品質スコアは、ユーザーと WhatsApp ユーザー間の会話からの品質シグナルの組み合わせに基づいて計算されます。これらのシグナルには、ブロック、レポート、ユーザーがビジネスをブロックするときに提供する理由などのユーザーフィードバックが含まれます。Meta は、最近のフィードバックとやり取りに焦点を当てながら WhatsApp、 で顧客が受け取ったメッセージの質を評価します。

WhatsApp 電話番号の品質評価

- 緑: 高品質
- 黄: 中品質
- 赤: 低品質

WhatsApp 電話番号のステータス

- 接続済み : メッセージ制限内でメッセージを送信できます。
- フラグ付き : 電話番号の品質が低く、改善する必要があります。7 日以内に電話の品質が改善しない場合、電話番号のステータスは Connected に変更されますが、ビジネス主導の会話の制限は 1 階層低くなります。
- 制限付き : 現在の 24 時間、ビジネス主導の会話の制限に達しましたが、受信カスタマーメッセージに応答することはできます。24 時間が終了したら、メッセージを再度送信できます。

電話番号の品質評価を表示する

電話番号の品質を表示するには、次の指示に従います。

1. で AWS エンドユーザーメッセージングソーシャルコンソールを開きますhttps://console.aws.amazon.com/social-messaging/。
2. ビジネスアカウントでは、 を選択しますWABA。
3. 電話番号タブには、電話番号、表示名、品質評価、その日に残したビジネス開始の会話の数が表示されます。

AWS エンドユーザーメッセージングソーシャルでのメッセージテンプレートの使用

週刊ニュースレターや予約リマインダーなど、頻繁に使用するメッセージタイプにメッセージテンプレートを使用できます。テンプレートメッセージは、まだメッセージを送信していないお客様、または過去 24 時間以内にメッセージを送信していないお客様に送信できる唯一のタイプのメッセージです。

メタは、各テンプレートに品質評価とステータスを割り当てます。品質評価は、テンプレートのステータスに影響を与え、テンプレートのペーシングまたは送信レートを下げます。

テンプレートは WhatsApp ビジネスアカウント (WABA) に関連付けられ、 WhatsApp マネージャーを通じて管理され、 によって確認されます WhatsApp。

次のテンプレートタイプを送信できます。

- テキストベース
- メディアベース
- インタラクティブメッセージ
- ロケーションベース
- ワンタイムパスワードボタンを使用した認証テンプレート
- マルチ製品メッセージテンプレート

Meta には、事前に承認されたサンプルテンプレートが用意されています。詳細については、「メッセージテンプレートのサンプル」を参照してください。

メッセージテンプレートのタイプの詳細については、 WhatsApp ビジネスプラットフォームクラウドAPIリファレンスの「メッセージテンプレート」を参照してください。

Manager での WhatsAppメッセージテンプレートの使用

WhatsApp マネージャーを使用して、テンプレートのステータスを作成、変更、または確認します。

1. で AWS エンドユーザーメッセージングソーシャルコンソールを開きますhttps://console.aws.amazon.com/social-messaging/。
2. ビジネスアカウント を選択し、 を選択しますWABA。

3. メッセージテンプレートタブで、メッセージテンプレートの管理 を選択します。WhatsApp マネージャーが新しいウィンドウで開き、メッセージテンプレート を選択してテンプレートを管理できます。

次のステップ

テンプレートを作成または編集したら、 で確認できるように送信する必要がありますWhatsApp。Meta のレビューには最大 24 時間かかる場合があります。Meta は Business Manager 管理者に E メールを送信し、 WhatsApp マネージャーのテンプレートステータスを更新します。WhatsApp マネージャーを使用してテンプレートのステータスを確認します。

でのテンプレートペーシングについて WhatsApp

テンプレートのペーシングは、Meta が使用する方法で、新規または変更されたテンプレートに関する顧客からの早期フィードバックに時間をかけることができます。エンゲージメントやフィードバックが不十分なテンプレートを識別して一時停止するため、テンプレートコンテンツをあまりにも多くの顧客に送信する前に調整する時間を確保できます。これにより、ビジネスに影響を与えるネガティブな顧客フィードバックのリスクが軽減されます。例えば、メッセージを「ブロック」する顧客が多すぎる場合や、テンプレートの読み取りレートが低い場合、テンプレートの品質評価を下げることができます。

テンプレートのペーシングは、新しく作成されたテンプレート、一時停止されていないテンプレート、および高品質の評価のないテンプレートに影響します。テンプレートのペーシングは、多くの場合、低品質または一時停止されたテンプレートの以前の履歴によって開始されます。テンプレートがペース調整されると、そのテンプレートを使用するメッセージは通常、Meta によって決定される特定のしきい値まで送信されます。その後、後続のメッセージは保持され、お客様のフィードバックに時間をかけることができます。フィードバックが正の場合、テンプレートのペーシングはスケールアップされます。フィードバックが負の場合、テンプレートのペースは低下するため、テンプレートの内容を調整できます。詳細については、 WhatsApp ビジネスプラットフォームクラウドAPIリファレンス の「テンプレートペーシング」を参照してください。

WhatsApp Manager でテンプレートのステータスが下がったことに関するフィードバックを取得する

Meta は、テンプレートのステータスが低下した理由に関する情報を提供します。Meta からのフィードバックを使用してテンプレートを編集し、再承認のために送信するか、別のテンプレートを使用す

るか、アプリケーションの動作を変更します。メッセージテンプレートを編集して再承認すると、頻繁な否定的なフィードバックや低い読み取り率を受け取らない限り、品質評価は徐々に向上します。

1. で AWS エンドユーザーメッセージングソーシャルコンソールを開きますhttps://console.aws.amazon.com/social-messaging/。
2. ビジネスアカウント を選択し、 を選択しますWABA。
3. メッセージテンプレートタブで、メッセージテンプレートの管理 を選択します。WhatsApp マネージャーが新しいウィンドウで開きます。
4. メッセージテンプレート を選択し、テンプレートにカーソルを合わせます。評価が低下した理由に関するフィードバックを含むツールヒントが表示されます。

でのテンプレートのステータスと品質評価について WhatsApp

各メッセージテンプレートには、使用状況、顧客のフィードバック、カスタマーエンゲージメントに基づいて品質評価が割り当てられます。テンプレートは、ステータスがアクティブである場合にのみ使用できますが、品質によってテンプレートのペーシングが決まります。メッセージテンプレートが一貫して否定的なフィードバックを受け取ったり、エンゲージメントが低下したりすると、テンプレートのステータスが変更されます。

メタは、否定的または肯定的なフィードバックとエンゲージメントに基づいて、テンプレートのステータスまたは品質評価を自動的に変更します。テンプレートのステータスが変更されると、WhatsApp マネージャー通知、E メール、イベント通知が送信されます。WhatsApp マネージャーを使用してテンプレートのステータスを確認します。

テンプレートが によって拒否された場合は WhatsApp、テンプレートを編集し、承認のために再送信するか、 に異議申し立てを提出できます WhatsApp。詳細については、WhatsApp 「 Business Platform Cloud API Reference」の「Appeals」を参照してください。

[テンプレートのステータス]	品質評価	意味
レビュー中		メッセージテンプレートはレビュー中です。これには最大 24 時間かかる場合があります。

[テンプレートのステータス]	品質評価	意味
拒否		メッセージテンプレートが拒否され、アピールを申請できます。
[アクティブ]	保留中	メッセージテンプレートは、お客様から品質フィードバックやリードレート情報を受信していませんが、メッセージの送信にも使用できます。
[アクティブ]	高い	メッセージテンプレートは、ネガティブな顧客フィードバックをほとんどまたはまったく受け取っていないため、メッセージの送信に使用できます。
[アクティブ]	中程度	メッセージテンプレートは、顧客から否定的なフィードバックを受け取ったか、読み取りレートが低く、一時停止またはオフになっている可能性があります。

[テンプレートのステータス]	品質評価	意味
[アクティブ]	低	メッセージテンプレートは、顧客から否定的なフィードバック、または低い読み取りレートを受信しました。このステータスのメッセージテンプレートを使用できますが、一時停止または無効化されるリスクがあります。 テンプレートがアクティブ/低ステータスに移行すると、送信は一時停止されます。最初の一時停止は 3 時間、2 番目の一時停止は 6 時間で、次の一時停止はテンプレートを無効にします。
一時停止中		メッセージテンプレートは、お客様からの否定的なフィードバックが繰り返し発生するか、読み取りレートが低いため一時停止されました。
無効		お客様からの否定的なフィードバックが繰り返し発生するため、メッセージテンプレートは無効になっています。
リクエストされた上訴		アピールがリクエストされました。

でテンプレートが拒否される理由 WhatsApp

メッセージテンプレートが Meta によってレビューおよび拒否されると、テンプレートが拒否された理由を説明する E メールが送信されます。拒否を申し立てるか、メッセージテンプレートを変更できます。以下は、Meta がメッセージテンプレートを拒否する一般的な理由の一部です。

- 変数パラメータには、#、$、% などの特殊文字が含まれます。
- 可変パラメータが欠落しているか、中括弧が一致していないか、シーケンシャルではありません。
- メッセージテンプレートには、WhatsApp コマースポリシー または WhatsApps ビジネスポリシー に違反するコンテンツが含まれています。

詳細については、 WhatsApp ビジネスプラットフォームクラウドAPIリファレンスの「一般的な拒否理由」を参照してください。

AWS エンドユーザーメッセージングソーシャルのメッセージとイベントの送信先

イベント送信先は、 WhatsApp イベントが送信される Amazon SNSトピックです。Amazon SNSトピックへのイベント発行を有効にすると、すべての送受信イベントが Amazon SNSトピックに送信されます。イベントを使用して、アウトバウンドメッセージと受信カスタマー通信のステータスをモニタリング、追跡、分析します。

各 WhatsApp ビジネスアカウント (WABA) には 1 つのイベント送信先を設定できます。 WhatsApp ビジネスアカウントに関連付けられたすべてのリソースからのすべてのイベントは、そのイベント送信先にログに記録されます。例えば、3 つの電話番号が関連付けられている WhatsApp ビジネスアカウントがあり、それらの電話番号からのすべてのイベントが 1 つのイベント送信先にログ記録されているとします。

トピック

- メッセージとイベントの宛先を AWS エンドユーザーメッセージングソーシャルに追加する
- AWS End User Messaging Social のメッセージとイベント形式
- WhatsApp メッセージステータス

メッセージとイベントの宛先を AWS エンドユーザーメッセージングソーシャルに追加する

メッセージとイベントの発行を有効にすると、 WhatsApp ビジネスアカウント (WABA) によって生成されたすべてのイベントが Amazon SNSトピックに送信されます。これには、 WhatsApp ビジネスアカウントに関連付けられた各電話番号のイベントが含まれます。にはWABA、1 つの Amazon SNSトピックを関連付けることができます。

前提条件

開始する前に、以下の前提条件を満たす必要があります。

- （オプション）AWS KMS キーを使用して暗号化された Amazon SNSトピックを使用するには、既存のキーポリシー に AWS エンドユーザーメッセージングソーシャルアクセス許可を付与する必要があります。

メッセージとイベントの宛先を追加する

1. で AWS エンドユーザーメッセージングソーシャルコンソールを開きますhttps://console.aws.amazon.com/social-messaging/。
2. ビジネスアカウント を選択し、 を選択しますWABA。
3. イベント送信先タブで、送信先の編集 を選択します。
4. イベントの送信先を有効にするには、 を有効にする を選択します。
5. イベントを新しい Amazon SNS送信先に送信するには、新しいSNSスタンドトピック を選択し、トピック名 に名前を入力します。Amazon SNSトピックは、 AWS エンドユーザーメッセージングソーシャルがトピックにアクセスすることを許可するアクセス許可で作成されます。

   既存の Amazon 送信SNS先にイベントを送信するには、既存のSNS標準トピック を選択し、トピックフォームトピック arn を選択します。Amazon SNSトピックには、次のアクセス許可を適用する必要があります。

   ```
   {
       "Effect": "Allow",
       "Principal": {
           "Service": [
             "social-messaging.amazonaws.com"
           ]
          },
       "Action": "sns:Publish",
       "Resource": "arn:{PARTITION}:sns:{REGION}:{ACCOUNT}:{TOPIC_NAME}"
   }
   ```

6. [Save changes] (変更の保存) をクリックします。

暗号化された Amazon SNSトピックポリシー

AWS KMS キーを使用して暗号化された Amazon SNSトピックを使用して、セキュリティを強化できます。このようなセキュリティの強化は、プライベートなデータや機密性の高いデータを扱うアプリケーションに有効です。 AWS KMS キーを使用した Amazon SNSトピックの暗号化の詳細については、「Amazon Simple Notification Service デベロッパーガイド」のAWS 「サービスからのイベントソースと暗号化されたトピック間の互換性を有効にする」を参照してください。

この例では、混乱した代理問題を回避するために、オプションですが推奨される SourceAccount および SourceArn条件を使用し、 AWS エンドユーザーメッセージングソーシャル所有者アカウン

トのみがアクセスできます。混乱した代理問題の詳細については、IAMユーザーガイドの「混乱した代理問題」を参照してください。

使用するキーは対称 である必要があります。暗号化された Amazon SNSトピックでは、非対称 AWS KMS キーはサポートされていません。

キーポリシーを変更して、 AWS エンドユーザーメッセージングソーシャルがキーを使用できるようにする必要があります。デAWS Key Management Service ベロッパーガイドの「キーポリシーの変更」の指示に従って、既存のキーポリシーに次のアクセス許可を追加します。

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "social-messaging.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{ACCOUNT_ID}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:{PARTITION}:social-messaging:{REGION}:{ACCOUNT_ID}:*"
        }
     }
}
```

次のステップ

Amazon SNSトピックを設定したら、エンドポイントをトピックにサブスクライブする必要があります。エンドポイントは、関連するトピックに発行されたメッセージを受信し始めます。トピックへのサブスクライブの詳細については、「Amazon デベロッパーガイド」の「Amazon SNSトピックへのサブスクライブ」を参照してください。 SNS

AWS End User Messaging Social のメッセージとイベント形式

イベントのJSONオブジェクトには、 AWS イベントヘッダーと WhatsApp JSONペイロードが含まれます。JSON WhatsApp 通知ペイロードと値のリストについては、WhatsApp Business Platform

Cloud Reference のAPI「Webhooks Notification Payload Reference」と「Message Status」を参照してください。

AWS エンドユーザーメッセージングソーシャルイベントヘッダー

イベントのJSONオブジェクトには、 AWS イベントヘッダーと が含まれます WhatsApp JSON。ヘッダーには、 WhatsApp ビジネスアカウント (WABA) ARNsの AWS 識別子と電話番号が含まれます。

```
{
  "MetaWabaIds": [
    {
      "wabaId": "1234567890abcde",
      "arn": "arn:aws:social-messaging:us-
east-1:123456789012:waba/fb2594b8a7974770b128a409e2example"
    }
  ],
  "MetaPhoneNumberIds": [
    {
      "metaPhoneNumberId": "abcde1234567890",
      "arn": "arn:aws:social-messaging:us-east-1:123456789012:phone-number-
id/976c72a700aac43eaf573ae050example"
    }
  ]
}
{
//WhatsApp notification payload
}
```

前の例のイベントでは、次のようになります。

- *1234567890abcde* は Meta の WABA ID です。
- *abcde1234567890* は Meta の電話番号 ID です。
- *fb2594b8a7974770b128a409e2example* は WhatsApp ビジネスアカウント () の ID です WABA。
- *976c72a700aac43eaf573ae050example* は電話番号の ID です。

テキストメッセージの受信例 WhatsApp JSON

からのテキストメッセージのイベントレコードを次に示します WhatsApp。JSON は によって生成されます WhatsApp。フィールドとその意味のリストについては、 ビジネスプラットフォームクラウドリファレンス の「Webhooks Notification Payload Reference」を参照してください。 WhatsApp API

```
{
//AWS End User Messaging Social header
}
{
  "id": "365731266123456",
  "changes": [
    {
      "value": {
        "messaging_product": "whatsapp",
        "metadata": {
          "display_phone_number": "12065550100",
          "phone_number_id": "321010217760100"
        },
        "contacts": [
          {
            "profile": {
              "name": "Diego"
            },
            "wa_id": "12065550102"
          }
        ],
        "messages": [
          {
            "from": "14255550150",
            "id":
 "wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjVGRkexample",
            "timestamp": "1723506035",
            "text": {
              "body": "Hi"
            },
            "type": "text"
          }
        ]
      },
      "field": "messages"
    }
```

```
  ]
}
```

メディアメッセージを受信する例 WhatsApp JSON

受信メディアメッセージのイベントレコードを次に示します。メディアファイルを取得するには、コマンドを使用します GetWhatsAppMessageMedia API。フィールドとその意味のリストについては、「Webhooks Notification Payload Reference」を参照してください。

```
{
//AWS End User Messaging Social header
}
{
  "id": "365731266123456",
  "changes": [
    {
      "value": {
        "messaging_product": "whatsapp",
        "metadata": {
          "display_phone_number": "12065550100",
          "phone_number_id": "321010217760100"
        },
        "contacts": [
          {
            "profile": {
              "name": "Diego"
            },
            "wa_id": "12065550102"
          }
        ],
        "messages": [
          {
            "from": "14255550150",
            "id":
 "wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjVGRkexample",
            "timestamp": "1723506230",
            "type": "image",
            "image": {
              "mime_type": "image/jpeg",
              "sha256": "BTD0xlqSZ7l02o+/upusiNStlEZhA/urkvKf143Uqjk=",
              "id": "530339869524171"
            }
          }
```

```
        ]
      },
      "field": "messages"
    }
  ]
}
```

WhatsApp メッセージステータス

メッセージを送信すると、メッセージに関するステータスの更新が表示されます。これらの通知を受信するには、イベントログを有効にする必要があります。「」を参照してくださいAWS エンドユーザーメッセージングソーシャルのメッセージとイベントの送信先。

メッセージステータス

次の表には、考えられるメッセージステータスが含まれています。

ステータス名	説明
削除済み	カスタマーはメッセージを削除し、サーバーにダウンロードされた場合もメッセージを削除する必要があります。
配信済み	メッセージは正常に顧客に配信されました。
失敗	メッセージの送信に失敗しました。
read	顧客がメッセージを読みました。このステータスは、顧客が読み取り受信を有効にした場合にのみ送信されます。
送信済み	メッセージは送信されましたが、転送中です。
warning	メッセージには、使用できない、または存在しない項目が含まれています。

追加リソース

詳細については、 ビジネスプラットフォームクラウドリファレンスの「メッセージステータス」を参照してください。 WhatsApp API

で送信するメディアファイルのアップロード WhatsApp

メディアファイルを送受信するときは、Amazon S3 バケットに保存する必要があります。Amazon S3 バケットは、 WhatsApp ビジネスアカウント () AWS リージョン と同じ AWS アカウント と にある必要がありますWABA。これらの指示は、Amazon S3 バケットの作成、ファイルのアップロード、および の ファイルURLへのビルドの方法を示しています。Amazon S3 コマンドの詳細については、「 で高レベル (s3) コマンドを使用する」を参照してくださいAWSCLI。の設定の詳細については AWS CLI、AWS Command Line Interface 「 ユーザーガイドAWS」の「 の設定CLI」、「バケットの作成」、Amazon S3 ユーザーガイド」の「オブジェクトのアップロード」を参照してください。

メディアファイルに署名付き URL を作成することもできます。署名付き を使用するとURL、他の当事者に AWS セキュリティ認証情報やアクセス許可を必要とせずに、オブジェクトへの時間制限付きアクセスを許可し、アップロードできます。

Amazon S3 バケットを作成するには、create-bucket AWS CLI コマンドを使用します。コマンドラインで以下のコマンドを入力します。

```
aws s3api create-bucket --region 'us-east-1' --bucket BucketName
```

上記のコマンドでは:

- 置換 *us-east-1* がWABA属 AWS リージョン する を使用します。
- 置換 *BucketName* 新しいバケットの名前。

Amazon S3 バケットにファイルをコピーするには、cp AWS CLI コマンドを使用します。コマンドラインで以下のコマンドを入力します。

```
aws s3 cp SourceFilePathAndName s3://BucketName/FileName
```

上記のコマンドでは:

- 置換 *SourceFilePathAndName* ファイルパスとコピーするファイルの名前。
- 置換 *BucketName* バケットの名前。
- 置換 *FileName* ファイルに使用する名前。

送信時に使用する URL は次のとおりです。

```
s3://BucketName/FileName
```

署名付き URLを作成するには、*user input placeholders* 独自の情報。

```
aws s3 presign s3://amzn-s3-demo-bucket1/mydoc.txt --expires-in 604800 --region af-south-1 --endpoint-url https://s3.af-south-1.amazonaws.com
```

返URLされる は次のとおりです。 `https://amzn-s3-demo-bucket1.s3.af-south-1.amazonaws.com/mydoc.txt?{Headers}`

でサポートされているメディアファイルの種類とサイズ WhatsApp

メディアメッセージを送受信する場合、ファイルタイプは最大ファイルサイズでサポートされる必要があります。詳細については、 WhatsApp ビジネスプラットフォームクラウドAPIリファレンスの「サポートされているメディアタイプ」を参照してください。

メディアファイルタイプ

オーディオ形式

オーディオタイプ	拡張機能	MIME タイプ	Max Size
AAC	.aac	audio/aac	16 MB
AMR	.amr	audio/amr	16 MB
MP3	.mp3	audio/mpeg	16 MB
MP4 オーディオ	.m4a	audio/mp4	16 MB
OGG オーディオ	.ogg	audio/ogg	16 MB

ドキュメント形式

ドキュメントタイプ	拡張機能	MIME タイプ	Max Size
テキスト	.text	text/plain	100 MB
Microsoft Excel	.xls、.xlsx	application/vnd.ms-excel、application/	100 MB

ドキュメントタイプ	拡張機能	MIME タイプ	Max Size
		vnd.openxmlformats-officedocument.spreadsheetml.sheet	
Microsoft Word	.doc、.docx	application/msword、application/vnd.openxmlformats-officedocument.wordprocessingml.document	100 MB
Microsoft PowerPoint	.ppt、.pptx	application/vnd.ms-powerpoint、application/vnd.openxmlformats-officedocument.presentationml.presentation	100 MB
PDF	.pdf	アプリケーション/pdf	100 MB

イメージ形式

イメージタイプ	拡張機能	MIME タイプ	Max Size
JPEG	.jpeg	image/jpeg	5 MB
PNG	.png	image/png	5 MB

ステッカー形式

ステッカータイプ	拡張機能	MIME タイプ	Max Size
アニメーションステッカー	.webp	image/webp	500 KB
静的ステッカー	.webp	image/webp	100 KB

ビデオ形式

ビデオタイプ	拡張機能	MIME タイプ	Max Size
3GPP	.3gp	ビデオ/3gp	16 MB
MP4 ビデオ	.mp4	video/mp4	16 MB

WhatsApp メッセージタイプ

このトピックでは、サポートされているメッセージタイプとその使用について説明します。メッセージタイプのリストについては、WhatsApp 「ビジネスプラットフォームクラウドAPIリファレンス」の「メッセージ」を参照してください。

メッセージの種類	説明
テキスト	テキストメッセージまたは URLを顧客に送信する
メディア	オーディオ、ドキュメント、イメージ、ステッカー、またはビデオファイルを送信します。メディアファイルのリンクを送信することもできます。
Reaction	絵文字をサムアップなどのメッセージへの反応として送信する
テンプレート	テンプレートメッセージを送信する
ロケーション	ロケーションを送信する
問い合わせ	問い合わせカードを送信する
インタラクティブ	インタラクティブメッセージを送信する

追加リソース

WhatsApp メッセージオブジェクトのリストについては、 WhatsApp ビジネスプラットフォームクラウドAPIリファレンスの「メッセージ」を参照してください。

AWS エンドユーザーメッセージングソーシャル WhatsApp を使用した からのメッセージの送信

メッセージを送信する前に、 のセットアップを完了WABAし、ユーザーがユーザーからのメッセージを受信するにはオプトインしている必要があります。「」を参照してください許可を取得する。

ユーザーからメッセージを受け取ると、カスタマーサービスウィンドウと呼ばれる 24 時間タイマーが起動または更新されます。テンプレートメッセージを除くすべてのメッセージタイプは、ユーザーとユーザーの間でカスタマーサービスウィンドウが開いている場合にのみ、ユーザーに送信できます。テンプレートメッセージは、ユーザーがユーザーからのメッセージの受信をオプトインしている限り、いつでもユーザーに送信できます。

メッセージステータスを送受信するメッセージごとに生成され、イベント送信先に送信されます。お客様がイベントにサインアップしていない場合 WhatsApp 、メッセージステータスは で生成されますfail。メッセージステータス を受信するには、メッセージとイベントの宛先を有効にする必要があります。

> **Important**
>
> Meta/ の使用WhatsApp
>
> - お客様による WhatsApp ビジネスソリューションの使用には、 WhatsApp サービス利用規約 、 WhatsApp ビジネスソリューション利用規約 、 WhatsApp ビジネスメッセージングポリシー 、 WhatsApp メッセージングガイドライン の利用規約、およびそれらに参照として組み込まれているその他のすべての条件、ポリシー、またはガイドライン (それぞれが随時更新される場合があります) が適用されます。
> - Meta または WhatsApp は、いつでも WhatsApp ビジネスソリューションの使用を禁止することができます。
> - WhatsApp ビジネスソリューションの使用に関連して、お客様は、適用される法律や規制に従って、配布の保護や制限の対象となるコンテンツ、情報、またはデータを送信しません。

トピック

- AWS End User Messaging Social でテンプレートメッセージを送信する例
- AWS End User Messaging Social でメディアメッセージを送信する例

AWS End User Messaging Social でテンプレートメッセージを送信する例

次の例は、 テンプレートを使用して を使用して顧客にメッセージを送信する方法を示しています AWS CLI。の設定の詳細については AWS CLI、 AWS Command Line Interface ユーザーガイドの「の設定 AWS CLI」を参照してください。

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","to":"'{PHONE_NUMBER}'","type":"template","template":
{"name":"statement","language":{"code":"en_US"},"components":
[{"type":"body","parameters":[{"type":"text","text":"1000"}]}]}}' --origination-phone-
number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version v20.0
```

上記のコマンドで、次の操作を行います。

- 置換 *{PHONE_NUMBER}* 顧客の電話番号を使用します。
- 置換 *{ORIGINATION_PHONE_NUMBER_ID}* 電話番号の ID を使用します。

AWS End User Messaging Social でメディアメッセージを送信する例

次の例は、 を使用して顧客にメディアメッセージを送信する方法を示しています AWS CLI。の設定の詳細については AWS CLI、 AWS Command Line Interface ユーザーガイドの「 の設定 AWS CLI」を参照してください。サポートされているメディアファイルタイプのリストについては、「」を参照してくださいでサポートされているメディアファイルの種類とサイズ WhatsApp。

1. メディアファイルを Amazon S3 バケットにアップロードします。「」を参照してくださいで送信するメディアファイルのアップロード WhatsApp。
2. post-whatsapp-message-media コマンド WhatsApp を使用して、メディアファイルを にアップロードします。正常に完了すると、 コマンドは を返します。*{MEDIA_ID}* メディアメッセージを送信するために必要です。

   ```
   aws socialmessaging post-whatsapp-message-media --origination-
   phone-number-id {ORIGINATION_PHONE_NUMBER_ID}  --source-s3-file
    bucketName={BUCKET},key={MEDIA_FILE}
   ```

   上記のコマンドで、次の操作を行います。

- 置換 *{ORIGINATION_PHONE_NUMBER_ID}* 電話番号の ID を使用します。
- 置換 *{BUCKET}* Amazon S3 バケットの名前。
- 置換 *{MEDIA_FILE}* メディアファイルの名前。

また、 --source-s3-presigned-url の代わりに を使用して、事前署名 URL を使用してアップロードすることもできます--source-s3-file。Content-Type ヘッダーフィールドに を追加する必要があります。両方を使用すると、 InvalidParameterExceptionが返されます。

```
--source-s3-presigned-url headers={"Name":"Value"},url=https://BUCKET.s3.REGION/
MEDIA_FILE
```

3. send-whatsapp-message コマンドを使用してメディアメッセージを送信します。

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","to":"'{PHONE_NUMBER}'","type":"image","image":
{"id":"'{MEDIA_ID}'"}}' --origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID}
 --meta-api-version v20.0
```

上記のコマンドで、次の操作を行います。

- 置換 *{PHONE_NUMBER}* 顧客の電話番号を使用します。
- 置換 *{ORIGINATION_PHONE_NUMBER_ID}* 電話番号の ID を使用します。
- 置換 *{MEDIA_ID}* 前のステップから返されたメディア ID を使用します。

4. メディアファイルが不要になった場合は、 delete-whatsapp-message-media コマンド WhatsApp を使用してメディアファイルを削除できます。これにより、Amazon S3 バケットではなく WhatsApp 、 からメディアファイルのみが削除されます。

```
aws socialmessaging delete-whatsapp-message-media --media-id {MEDIA_ID} --
origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID}
```

上記のコマンドで、次の操作を行います。

- 置換 *{ORIGINATION_PHONE_NUMBER_ID}* 電話番号の ID を使用します。
- 置換 *{MEDIA_ID}* メディア ID を使用します。

AWS End User Messaging Social で受信したメッセージへの応答

テキストまたはメディアメッセージを受信する前に、 の設定WABAとイベント送信先の設定を完了している必要があります。受信メッセージを受信すると、イベントはイベント送信先の Amazon SNSトピックに保存されます。通知を受け取るには、Amazon SNSトピックエンドポイントをサブスクライブする必要があります。

受信したメディアメッセージのイベント例については、「」を参照してくださいメディアメッセージを受信する例 WhatsApp JSON 。の設定の詳細については AWS CLI、 AWS Command Line Interface ユーザーガイドの「 の設定 AWS CLI」を参照してください。サポートされているメディアファイルタイプのリストについては、「」を参照してくださいでサポートされているメディアファイルの種類とサイズ WhatsApp。

> **Important**
>
> 受信メッセージを受信するにはWABA、 でイベント送信先が有効になっている必要があります。「」を参照してくださいメッセージとイベントの宛先を AWS エンドユーザーメッセージングソーシャルに追加する。

AWS End User Messaging Social で読み取るメッセージのステータスを変更する例

メッセージのステータスを に設定readして、エンドユーザーの画面に 2 つの青いチェックマークを表示できます。

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","message_id":"'{MESSAGE_ID}'","status":"read"}' --
origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version v20.0
```

上記のコマンドで、次の操作を行います。

- 置換 *{ORIGINATION_PHONE_NUMBER_ID}* 電話番号の ID を使用します。
- 置換 *{MESSAGE_ID}* メッセージの一意の識別子。Amazon SNSトピックのメッセージオブジェクトで idフィールドの値を使用します。

AWS End User Messaging Social でレスポンスを含むメッセージに応答する例

サムアップのように、メッセージにリアクションを追加できます。

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","recipient_type":"individual","to":"'{PHONE_NUMBER}'","type":
 "reaction","reaction": {"message_id": "'{MESSAGE_ID}'","emoji":"\uD83D\uDC4D"}}' --
origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version v20.0
```

上記のコマンドで、次の操作を行います。

- 置換 *{PHONE_NUMBER}* 顧客の電話番号で。
- 置換 *{MESSAGE_ID}* メッセージの一意の識別子。Amazon SNSトピックのメッセージオブジェクトで idフィールドの値を使用します。
- 置換 *{ORIGINATION_PHONE_NUMBER_ID}* 電話番号の ID を使用します。

から Amazon S3 WhatsApp にメディアファイルをダウンロードする

メディアファイルを取得して Amazon S3 バケットに保存するには、 get-whatsapp-message-media コマンドを使用します。

```
aws socialmessaging get-whatsapp-message-media --media-id {MEDIA_ID} --
origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --destination-s3-file
 bucketName={BUCKET},key=inbound_
{
    "mimeType": "image/jpeg",
    "fileSize": 78144
}
```

上記のコマンドで、次の操作を行います。

- 置換 *{BUCKET}* Amazon S3 バケットの名前。
- 置換 *{MEDIA_ID}* 受信したイベントからの ID フィールドの値。受信メディアイベントの例については、「」を参照してくださいメディアメッセージを受信する例 WhatsApp JSON 。
- 置換 *{ORIGINATION_PHONE_NUMBER_ID}* 電話番号の ID を使用します。

Amazon S3 バケットからメディアを取得するには、次のコマンドを使用します。

```
aws s3 cp s3://{BUCKET}/inbound_{MEDIA_ID}.jpeg
```

上記のコマンドで、次の操作を行います。

- 置換 *{BUCKET}* Amazon S3 バケットの名前。
- 置換 *{MEDIA_ID}* 前のステップから返された MEDIA_ID を使用します。

読み取りとリアクションでメッセージに応答する例

この例では、顧客である Diego から「Hi」というメッセージが送信され、読み取り受信とハンドウェーブ絵文字で返信しました。

前提条件

Diego がメッセージを送信した通知を受け取るには、イベント送信先 Amazon SNSトピックを設定し、トピックエンドポイントの 1 つをサブスクライブする必要があります。

応答

1. Diego からのメッセージが受信されると、トピックのエンドポイントにイベントが公開されます。以下は、トピックが公開する内容のスニペットです。

> **Note**
>
> Diego は会話を開始したため、ビジネス主導の会話にはカウントされません。

```
{
  "MetaWabaIds": [
    {
      "wabaId": "1234567890abcde",
      "arn": "arn:aws:social-messaging:us-east-1:123456789012:waba/
fb2594b8a7974770b128a409e2example"
    }
  ],
  "MetaPhoneNumberIds": [
    {
```

```
      "metaPhoneNumberId": "abcde1234567890",
      "arn": "arn:aws:social-messaging:us-east-1:123456789012:phone-number-
id/976c72a700aac43eaf573ae050example"
    }
  ]
}
  {
  "id": "365731266123456",
  "changes": [
    {
      "value": {
        "messaging_product": "whatsapp",
        "metadata": {
          "display_phone_number": "12065550100",
          "phone_number_id": "321010217712345"
        },
        "contacts": [
          {
            "profile": {
              "name": "Diego"
            },
            "wa_id": "12065550102"
          }
        ],
        "messages": [
          {
            "from": "14255550150",
            "id":
 "wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjVGRkexample",
            "timestamp": "1723506035",
            "text": {
              "body": "Hi"
            },
            "type": "text"
          }
        ]
      },
      "field": "messages"
    }
  ]
}
```

2. Diego を表示するには、 ステータスを に設定しますread。Diego は、デバイスのメッセージの横にある 2 つの青いチェックマークを表示します。

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","message_id":"'{MESSAGE_ID}'","status":"read"}'
 --origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version
 v20.0
```

上記のコマンドで、次の操作を行います。

- 置換 *{ORIGINATION_PHONE_NUMBER_ID}* Diego が にメッセージを送信した電話番号 IDphone-number-id-976c72a700aac43eaf573ae050example。
- 置換 *{MESSAGE_ID}* メッセージの一意の識別子。これは、受信したメッセージ の ID の値と同じで すwamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjVGRkex

3. Diego にハンドウェーブリアクションを送信できます。

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","recipient_type":"individual","to":"'{PHONE_NUMBER}'","ty
 "reaction","reaction": {"message_id": "'{MESSAGE_ID}'","emoji":"\uD83D\uDC4B"}}'
 --origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version
 v20.0
```

上記のコマンドで、次の操作を行います。

- 置換 *{PHONE_NUMBER}* Diego の電話番号 。 14255550150
- 置換 *{MESSAGE_ID}* メッセージの一意の識別子。これは、受信したメッセージ の ID の値と同じで すwamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjVGRkex
- 置換 *{ORIGINATION_PHONE_NUMBER_ID}* Diego が にメッセージを送信した電話番号 IDphone-number-id-976c72a700aac43eaf573ae050example。

追加リソース

- イベントの送信先を有効にして、イベントを記録し、受信メッセージを受信します。
- メッセージオブジェクトのリスト WhatsAppについては、 WhatsApp ビジネスプラットフォームクラウドAPIリファレンスの「メッセージ」を参照してください。

AWS エンドユーザーメッセージングソーシャルの WhatsApp 請求と使用状況レポートについて

AWS エンドユーザーメッセージングソーシャルチャネルは、次の形式の 5 つのフィールドを含む使用タイプを生成します。 *Region code*-*MessagingType*-*ISO*-*FeeDescription*-*FeeType* WhatsApp 会話 WhatsAppごとに 2 つの請求項目がありConversationFee、 AWS ごとに がありますMessageFee。

テンプレートメッセージを送信して会話を開始すると、 AWS ごとに 1 WhatsApp ConversationFeeつと 1 つの料金が請求されますMessageFee。これにより、24 時間ウィンドウが開き、同じ顧客から送受信する各メッセージは、 AWS ごとに として請求されますMessageFee。

WhatsApp 会話タイプと料金の詳細については、WhatsApp ビジネスプラットフォームデベロッパーガイドの「会話ベースの料金」を参照してください。

次の表は、使用タイプのフィールドに設定できる値と説明を示しています。 AWS エンドユーザーメッセージングソーシャルの料金の詳細については、AWS 「エンドユーザーメッセージングの料金」を参照してください。

フィールド	オプション	説明
Region code	• USE1 – 米国東部 (バージニア北部) リージョン • USE2 – 米国東部 (オハイオ) リージョン • USW1 – 米国西部 (オレゴン) リージョン • APS1 – アジアパシフィック (ムンバイ) リージョン • APSE1 – アジアパシフィック (シンガポール) リージョン • EUW1 – 欧州 (アイルランド) リージョン	WhatsApp メッセージの送受信元を示す AWS リージョンプレフィックス。

フィールド	オプション	説明
	• EUW2 – 欧州 (ロンドン) リージョン	
MessagingType	WhatsApp	このフィールドは、送信されるメッセージタイプを識別します。
ISO	サポートされている国を参照してください。	メッセージが送信された 2 桁のISO国コード。
FeeDescription	ConversationFee , MessageFee	このフィールドでは、WhatsApp ConversationFee AWS ごとに または を指定しますMessageFee 。

フィールド	オプション	説明
FeeType	Authentication , Marketing , Service, Utility, Standard	このフィールドには、使用された会話タイプのタイプが表示されるか、メッセージあたりの料金の標準を指定します。 ビジネス開始**ConversationFee** カテゴリ • Marketing – 意識の向上から、販売の促進、顧客の再ターゲット化まで、幅広い目標を達成するために使用されます。例としては、新製品、サービス、または機能の発表、ターゲットを絞ったプロモーション/オファー、カート放棄のリマインダーなどがあります。 • Utility – ユーザーアクションまたはリクエストのフォローアップに使用されます。例としては、オプトインの確認、注文/配送管理 (配送の更新など) 、アカウントの更新やアラート (支払いリマインダーなど) 、フィードバック調査などがあります。 • Authentication – ログインプロセスの複数のステップ (アカウント検証、アカウント復旧、整合性の課題など) で、ワンタイムパスコードを使用してユーザー

フィールド	オプション	説明
		を認証するために使用されます。 • Service – 顧客の問い合わせを解決するために使用されます。 ユーザー開始**ConversationFee** カテゴリ • Service – 顧客の問い合わせを解決するために使用されます。 **MessageFee** カテゴリ • Standard – 送受信されたメッセージあたりの料金。

テンプレートメッセージを送信して会話を開始すると、1 つの ConversationFeeと に対して請求されますMessageFee。これにより、24 時間ウィンドウが開き、同じ顧客に送信する各テンプレートメッセージが個別の として請求されますMessageFee。24 時間ウィンドウの間、テンプレートメッセージは同じタイプにする必要があります。そうしないと、新しい会話が開始されます。

例えば、マーケティングテンプレートメッセージを顧客に送信すると、 ConversationFeeと に対して請求されますMessageFee。

```
Marketing Template Message 1: APS1-WhatsApp-CA-ConversationFee-Marketing
Marketing Template Message 1: APS1-WhatsApp-CA-MessageFee-Standard
Marketing Template Message 2: APS1-WhatsApp-CA-MessageFee-Standard
```

お客様がメッセージを送信して返信した場合、新しいService会話とメッセージを開くと料金が発生します。

```
Service Message 1: APS1-WhatsApp-CA-ConversationFee-Service
Service Message 1: APS1-WhatsApp-CA-MessageFee-Standard
```

```
Service Message 2: APS1-WhatsApp-CA-MessageFee-Standard
Service Message 3: APS1-WhatsApp-CA-MessageFee-Standard
```

例 1: マーケティングテンプレートメッセージの送信

例えば、マーケティングテンプレートメッセージを顧客に送信すると、 AWS ごとに 1 WhatsApp ConversationFee つと 1 つの料金が請求されますMessageFee。

```
Marketing Template Message 1: APS1-WhatsApp-CA-ConversationFee-Marketing
Marketing Template Message 1: APS1-WhatsApp-CA-MessageFee-Standard
```

例 2: サービス会話を開く

サービス会話料金は、ビジネスによって開始されたアクティブな 24 時間会話ウィンドウの範囲外にあるユーザーのインバウンドメッセージにビジネスが応答する場合に適用されます。このシナリオでは、インバウンドメッセージとアウトバウンドメッセージごとに 1 WhatsApp ConversationFee つと AWS MessageFeeが請求されます。

```
Service Message 1: APS1-WhatsApp-CA-ConversationFee-Service
Service Message 1: APS1-WhatsApp-CA-MessageFee-Standard
Service Message 2: APS1-WhatsApp-CA-MessageFee-Standard
Service Message 3: APS1-WhatsApp-CA-MessageFee-Standard
```

AWS エンドユーザーメッセージングのソーシャル請求ISOコードと WhatsApp 会話料金マッピング

サポートされている国

2 桁のISO国コード	国名	WhatsApp 会話請求リージョン
AF	アフガニスタン	アジアパシフィックのその他の地域
AX	アランド諸島	その他
AL	アルバニア	その他の中欧および東欧

2 桁のISO国コード	国名	WhatsApp 会話請求リージョン
DZ	アルジェリア	アフリカのその他の地域
AS	アメリカ領サモア	その他
AD	アンドラ	その他
AO	アンゴラ	アフリカのその他の地域
AI	アンギラ	その他
AQ	南極大陸	その他
AG	アンティグアバーブーダ	その他
AR	アルゼンチン	アルゼンチン
AM	アルメニア	その他の中欧および東欧
AQ	アルバ	その他
AC	アセンションアイランド	その他
AU	オーストラリア	アジアパシフィックのその他の地域
AT	オーストリア	その他の西ヨーロッパ
AZ	アゼルバイジャン	その他の中欧および東欧
BS	バハマ諸島	その他
BH	バーレーン	中東のその他の地域
BD	バングラデシュ	アジアパシフィックのその他の地域
BB	バルバドス	その他
BY	ベラルーシ	その他の中欧および東欧

2 桁のISO国コード	国名	WhatsApp 会話請求リージョン
BE	ベルギー	その他の西ヨーロッパ
BZ	ベリーズ	その他
BJ	ベニン	アフリカのその他の地域
BM	バミューダ	その他
BT	ブータン	その他
BO	ボリビア	その他のラテンアメリカ
BQ	ボネール	その他
BA	ボスニアヘルツェゴビナ	その他
BW	ボツワナ	アフリカのその他の地域
BV	ブーベ島	その他
BR	ブラジル	ブラジル
IO	英領インド洋地域	その他
VG	英領バージン諸島	その他
BN	ブルネイ・ダルサラーム	その他
BG	ブルガリア	その他の中欧および東欧
BF	BurkinaFaso	アフリカのその他の地域
BI	ブルンジ	アフリカのその他の地域
KH	カンボジア	アジアパシフィックのその他の地域
CM	カメルーン	アフリカのその他の地域

2 桁のISO国コード	国名	WhatsApp 会話請求リージョン
CA	カナダ	北米
CV	カーボベルデ	その他
KY	ケイマン諸島	その他
CF	中央アフリカ共和国	その他
TD	チャド	アフリカのその他の地域
CL	チリ	チリ
CN	中国	アジアパシフィックのその他の地域
CX	クリスマス島	その他
CC	ココス (キーリング) 諸島	その他
CO	コロンビア	コロンビア
KM	コモロ	その他
CG	コンゴ	その他
CD	コンゴ	アフリカのその他の地域
CK	クック諸島	その他
CR	コスタリカ	その他のラテンアメリカ
CI	コートジボワール	アフリカのその他の地域
HR	クロアチア	その他の中欧および東欧
CW	キュラソー	その他
CY	キプロス	その他

2 桁のISO国コード	国名	WhatsApp 会話請求リージョン
CZ	チェコ共和国	その他の中欧および東欧
DK	デンマーク	その他の西ヨーロッパ
DJ	ジブチ	その他
DM	ドミニカ	その他
DO	ドミニカ共和国	その他のラテンアメリカ
EC	エクアドル	その他のラテンアメリカ
EG	エジプト	エジプト
SV	エルサルバドル	その他のラテンアメリカ
GQ	赤道ギニア	その他
ER	エリトリア	アフリカのその他の地域
EE	エストニア	その他
ET	エチオピア	アフリカのその他の地域
FK	フォークランド諸島	その他
FO	フェロー諸島	その他
FJ	フィジー	その他
FI	フィンランド	その他の西ヨーロッパ
FR	フランス	フランス
GF	フランス領ギアナ	その他
PF	フランス領ポリネシア	その他
TF	フランス領南方・南極地域	その他

2 桁のISO国コード	国名	WhatsApp 会話請求リージョン
GA	ガボン	アフリカのその他の地域
GM	ガンビア	アフリカのその他の地域
GE	ジョージア	その他の中欧および東欧
DE	ドイツ	ドイツ
GH	ガーナ	アフリカのその他の地域
GI	ジブラルタル	その他
GR	ギリシャ	その他の中欧および東欧
GL	グリーンランド	その他
GD	グレナダ	その他
GP	グアドループ	その他
GU	グアム	その他
GT	グアテマラ	その他のラテンアメリカ
GG	ガーンジー代官管轄区	その他
GN	ギニア	その他
GW	ギニアビサウ	アフリカのその他の地域
GY	ガイアナ	その他
HT	ハイチ	その他のラテンアメリカ
HM	ヒアリングと McDonald 島	その他
HN	ホンジュラス	その他のラテンアメリカ

2 桁のISO国コード	国名	WhatsApp 会話請求リージョン
HK	香港	アジアパシフィックのその他の地域
hu	ハンガリー	その他の中欧および東欧
IS	アイスランド	その他
IN	インド	インド
IN	インドインターナショナル	インドインターナショナル
ID	インドネシア	インドネシア
ID	インドネシアインターナショナル	インドネシアインターナショナル
IQ	イラク	中東のその他の地域
IE	アイルランド	その他の西ヨーロッパ
IM	マン島	その他
IL	イスラエル	イスラエル
IT	イタリア	イタリア
JM	ジャマイカ	その他のラテンアメリカ
JP	日本	アジアパシフィックのその他の地域
JE	ジャージー	その他
JO	ヨルダン	中東のその他の地域
KZ	カザフスタン	その他
KE	ケニア	アフリカのその他の地域

2 桁のISO国コード	国名	WhatsApp 会話請求リージョン
KI	キリバス	その他
XK	コソボ共和国	その他
KW	クウェート	中東のその他の地域
KG	キルギスタン	その他
LA	ラオス PDR	アジアパシフィックのその他の地域
LV	ラトビア	その他の中欧および東欧
LB	レバノン	中東のその他の地域
LS	レソト	アフリカのその他の地域
LR	リベリア	アフリカのその他の地域
LY	リビア	アフリカのその他の地域
LI	リヒテンシュタイン	その他
LT	リトアニア	その他の中欧および東欧
LU	ルクセンブルグ	その他
MO	マカオ	その他
MK	マケドニア	その他の中欧および東欧
MG	マダガスカル	アフリカのその他の地域
MW	マラウイ	アフリカのその他の地域
MY	マレーシア	マレーシア
MV	モルジブ	その他

2 桁のISO国コード	国名	WhatsApp 会話請求リージョン
ML	マリ	アフリカのその他の地域
MT	マルタ	その他
MH	マーシャル諸島共和国	その他
MQ	マルチニーク	その他
MR	モーリタニア	アフリカのその他の地域
MU	モーリシャス	その他
YT	マヨット	その他
MX	メキシコ	メキシコ
FM	ミクロネシア	その他
MD	モルドバ	その他の中欧および東欧
MC	モナコ	その他
MN	モンゴル	アジアパシフィックのその他の地域
ME	モンテネグロ	その他
MS	モントセラト	その他
MA	モロッコ	アフリカのその他の地域
MZ	モザンビーク	アフリカのその他の地域
MM	ミャンマー	その他
該当なし	ナミビア	アフリカのその他の地域
NR	ナウル	その他

2 桁のISO国コード	国名	WhatsApp 会話請求リージョン
NP	ネパール	アジアパシフィックのその他の地域
NL	オランダ	オランダ
NC	ニューカレドニア	その他
NZ	ニュージーランド	アジアパシフィックのその他の地域
NI	ニカラグア	その他のラテンアメリカ
NE	ニジェール	アフリカのその他の地域
NG	ナイジェリア	ナイジェリア
NU	ニウエ	その他
NF	ノーフォーク島	その他
MP	北マリアナ諸島	その他
いいえ	ノルウェー	その他の西ヨーロッパ
OM	オマーン	中東のその他の地域
PK	パキスタン	パキスタン
PW	パラオ	その他
PS	パレスチナ	その他
PA	パナマ	その他のラテンアメリカ
PG	パプアニューギニア	アジアパシフィックのその他の地域
PY	パラグアイ	その他のラテンアメリカ

2 桁のISO国コード	国名	WhatsApp 会話請求リージョン
PE	ペルー	ペルー
PH	フィリピン	アジアパシフィックのその他の地域
PN	ピットケアン	その他
PL	ポーランド	その他の中欧および東欧
PT	ポルトガル	その他の西ヨーロッパ
PR	プエルトリコ	その他のラテンアメリカ
QA	カタール	中東のその他の地域
RE	レユニオン	その他
RO	ルーマニア	その他の中欧および東欧
RU	ロシア連邦	ロシア
RW	ルワンダ	アフリカのその他の地域
SH	セントヘレナ	その他
KN	セントクリストファーネイビス	その他
LC	セントルシア	その他
PM	サンピエール・ミクロン	その他
VC	セントビンセントとグレナディーン	その他
BL	サン・バルテレイミー	その他
MF	サンマーティン	その他

2 桁のISO国コード	国名	WhatsApp 会話請求リージョン
WS	サモア	その他
SM	サンマリノ	その他
ST	サントメプリンシペ	その他
SA	サウジアラビア	サウジアラビア
SN	セネガル	アフリカのその他の地域
RS	セルビア	その他の中欧および東欧
SC	セイシェル	その他
SL	シエラレオネ	アフリカのその他の地域
SG	シンガポール	アジアパシフィックのその他の地域
SX	シントマールテン	その他
SK	スロバキア	その他の中欧および東欧
SI	スロベニア	その他の中欧および東欧
SB	ソロモン諸島	その他
SO	ソマリア	アフリカのその他の地域
ZA	南アフリカ	南アフリカ
GS	サウスジョージア・サウスサンドウィッチ諸島	その他
KR	韓国	その他
SS	南スーダン	アフリカのその他の地域
ES	スペイン	スペイン

2 桁のISO国コード	国名	WhatsApp 会話請求リージョン
LK	スリランカ	アジアパシフィックのその他の地域
SR	スリナム	その他
SJ	スバーバル諸島とジャンマイン諸島	その他
SZ	スワジランド	アフリカのその他の地域
SE	スウェーデン	その他の西ヨーロッパ
CH	スイス	その他の西ヨーロッパ
TW	台湾	アジアパシフィックのその他の地域
TJ	タジキスタン	アジアパシフィックのその他の地域
TZ	タンザニア	アフリカのその他の地域
TH	タイ	アジアパシフィックのその他の地域
TL	東ティモール	その他
TG	トーゴ	アフリカのその他の地域
TK	トケラウ	その他
TO	トンガ	その他
TT	トリニダード・トバゴ	その他
TA	Trist と Cunha	その他
TN	チュニジア	アフリカのその他の地域

2 桁のISO国コード	国名	WhatsApp 会話請求リージョン
TR	トルコ	トルコ
TM	トルクメニスタン	アジアパシフィックのその他の地域
TC	タークスおよびカイコス諸島	その他
TV	ツバル	その他
UG	ウガンダ	アフリカのその他の地域
UA	ウクライナ	その他の中欧および東欧
AE	アラブ首長国連邦	アラブ首長国連邦
GB	英国	英国
米国	アメリカ	北米
UY	ウルグアイ	その他のラテンアメリカ
UM	米国マイナーアウトリーイング諸島	その他
UZ	ウズベキスタン	アジアパシフィックのその他の地域
VU	バヌアツ	その他
VA	バチカン市国	その他
VE	ベネズエラ	その他のラテンアメリカ
VN	ベトナム	アジアパシフィックのその他の地域
VI	バージン諸島	その他

2 桁のISO国コード	国名	WhatsApp 会話請求リージョン
WF	ウォリス諸島とフツナ諸島	その他
EH	西サハラ	その他
YE	イエメン	中東のその他の地域
ZM	ザンビア	アフリカのその他の地域
ZW	ジンバブエ	その他

AWS エンドユーザーメッセージングソーシャルのモニタリング

モニタリングは、 AWS エンドユーザーメッセージングソーシャルやその他のAWSソリューションの信頼性、可用性、パフォーマンスを維持する上で重要です。AWS には、 AWS エンドユーザーメッセージングソーシャルをモニタリングし、問題が発生したときに報告し、必要に応じて自動アクションを実行するための以下のモニタリングツールが用意されています。

- Amazon CloudWatch は AWS 、リソースと で実行するアプリケーションを AWS 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、Amazon EC2インスタンスのCPU使用状況やその他のメトリクス CloudWatch を追跡し、必要に応じて新しいインスタンスを自動的に起動できます。詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。
- Amazon CloudWatch Logs を使用すると、Amazon EC2インスタンスやその他のソースからログファイルをモニタリング、保存 CloudTrail、およびアクセスできます。 CloudWatch ログはログファイル内の情報をモニタリングし、特定のしきい値に達したときに通知できます。高い耐久性を備えたストレージにログデータをアーカイブすることもできます。詳細については、「Amazon CloudWatch Logs ユーザーガイド」を参照してください。
- AWS CloudTrail は、アカウントによって、または AWS アカウントに代わって行われたAPI呼び出しおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。と呼ばれるユーザーとアカウント AWS、呼び出し元の送信元 IP アドレス、呼び出しが発生した日時を特定できます。詳細については、AWS CloudTrail ユーザーガイドをご参照ください。

Amazon での AWS エンドユーザーメッセージングソーシャルのモニタリング CloudWatch

を使用して AWS エンドユーザーメッセージングソーシャルをモニタリングできます。これにより CloudWatch、生データが収集され、読み取り可能なほぼリアルタイムのメトリクスに処理されます。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、ウェブアプリケーションまたはサービスの動作をより的確に把握できます。また、特定のしきい値を監視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。

AWS End User Messaging Social では、 をモニタリングしWhatsAppMessageFeeCount、支出のしきい値に達したときにアラームをモニタリングWhatsAppConversationFeeCountしてトリガーすることもできます。

次の表に、 AWS エンドユーザーメッセージングソーシャルがAWS/SocialMessaging名前空間にエクスポートするメトリクスとディメンションを示します。

メトリクス	単位	説明
WhatsAppConversationFeeCount	カウント	WhatsApp 会話料金の数
WhatsAppMessageFeeCount	カウント	WhatsApp メッセージ料金の数

ディメンション	説明
MessageFeeType	有効な料金タイプは、サービス、マーケティング、ユーティリティ、認証です。
DestinationCountryCode	国の 2 文字のISOコード
WhatsAppPhoneNumberArn	電話番号のアーク

を使用した AWS エンドユーザーメッセージングソーシャルAPIコールのログ記録 AWS CloudTrail

AWS エンドユーザーメッセージングソーシャルは、ユーザーAWS CloudTrail、ロール、または によって実行されたアクションの記録を提供するサービスである と統合されています AWS のサービス。 は、 AWS エンドユーザーメッセージングソーシャルのすべてのAPI呼び出しをイベントとして CloudTrail キャプチャします。キャプチャされた呼び出しには、 AWS エンドユーザーメッセージングソーシャルコンソールからの呼び出しと AWS 、エンドユーザーメッセージングソーシャルAPIオペレーションへのコード呼び出しが含まれます。によって収集された情報を使用して CloudTrail、AWS エンドユーザーメッセージングソーシャルに対して行われたリクエスト、リクエスト元の IP アドレス、リクエスト日時、および追加の詳細を確認できます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます:

- ルートユーザーまたはユーザー認証情報のどちらを使用してリクエストが送信されたか
- リクエストが IAM Identity Center ユーザーに代わって行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービスによって送信されたかどうか。

CloudTrail は、アカウントを作成し、イベント履歴 に自動的にアクセスできる AWS アカウント ときに、 でアクティブになります。 CloudTrail CloudTrail イベント履歴には、過去 90 日間の で記録された管理イベントの表示可能、検索可能、ダウンロード可能、および変更不可能なレコードが表示されます AWS リージョン。詳細については、AWS CloudTrail 「 ユーザーガイド」の CloudTrail 「イベント履歴の操作」を参照してください。イベント履歴を表示するための料金は発生しません CloudTrail。

AWS アカウント 過去 90 日間のイベントを継続的に記録するには、証跡または CloudTrail Lake イベントデータストアを作成します。

CloudTrail 証跡

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。を使用して作成されたすべての証跡 AWS Management Console はマルチリージョンです。 AWS CLIを使用する際は、単一リージョンまたは複数リージョンの証跡を作成できます。アカウント AWS リージョン 内のすべての でアクティビティをキャプチャするため、マルチリージョン証跡を作成することをお勧めします。単一リージョンの証跡を作成する場合、証跡の AWS リージョンに記録されたイベントのみを表示できます。証跡の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS アカウントの証跡の作成」および「組織の証跡の作成」を参照してください。

証跡を作成 CloudTrail することで、進行中の管理イベントのコピーを から Amazon S3 バケットに無料で配信できますが、Amazon S3 ストレージ料金が発生します。 CloudTrail 料金の詳細については、AWS CloudTrail 「料金」を参照してください。Amazon S3 の料金に関する詳細については、「Amazon S3 の料金」を参照してください。

CloudTrail Lake イベントデータストア

CloudTrail Lake では、イベントに対して SQLベースのクエリを実行できます。 CloudTrail Lake は既存のイベントを行ベースのJSON形式で Apache ORC 形式に変換します。ORC は、データ

の高速取得用に最適化された列型ストレージ形式です。イベントはイベントデータストアに集約されます。イベントデータストアは、高度なイベントセレクタを適用することによって選択する条件に基いた、イベントのイミュータブルなコレクションです。どのイベントが存続し、クエリに使用できるかは、イベントデータストアに適用するセレクタが制御します。 CloudTrail Lake の詳細については、AWS CloudTrail 「 ユーザーガイド」のAWS CloudTrail 「Lake の使用」を参照してください。

CloudTrail Lake イベントデータストアとクエリにはコストがかかります。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。 CloudTrail 料金の詳細については、AWS CloudTrail 「料金」を参照してください。

AWS のエンドユーザーメッセージングソーシャルデータイベント CloudTrail

データイベントでは、リソース上またはリソース内で実行されるリソースオペレーション (Amazon S3 オブジェクトの読み取りまたは書き込みなど) についての情報が得られます。これらのイベントは、データプレーンオペレーションとも呼ばれます。データイベントは、多くの場合、高ボリュームのアクティビティです。デフォルトでは、 CloudTrail はデータイベントを記録しません。 CloudTrail イベント履歴にはデータイベントは記録されません。

追加の変更がイベントデータに適用されます。 CloudTrail 料金の詳細については、AWS CloudTrail 「料金」を参照してください。

CloudTrail コンソール、、または CloudTrail API オペレーションを使用して AWS CLI、 AWS エンドユーザーメッセージングソーシャルリソースタイプのデータイベントをログに記録できます。データイベントをログに記録する方法の詳細については、「 AWS CloudTrail ユーザーガイド」の「AWS Management Consoleを使用したデータイベントのログ記録」および「AWS Command Line Interfaceを使用したデータイベントのログ記録」を参照してください。

次の表に、データイベントをログ記録できる AWS エンドユーザーメッセージングソーシャルリソースタイプを示します。データイベントタイプ (コンソール) 列には、 CloudTrail コンソールのデータイベントタイプリストから選択する値が表示されます。resources.type 値列には、 AWS CLI または を使用して高度なイベントセレクタを設定するときに指定する`resources.type`値が表示されます CloudTrail APIs。にAPIs記録されたデータ CloudTrail列には、リソースタイプの CloudTrail に記録されたAPI呼び出しが表示されます。

データイベントタイプ (コンソール)	resources.type 値	にAPIs記録されたデータ CloudTrail
ソーシャルメッセージ電話番号 ID	`AWS::SocialMessaging::PhoneNumberId`	• DeleteWhatsAppMessageMedia • GetWhatsAppMessageMedia • PostWhatsAppMessageMedia • SendWhatsAppMessage

`eventName`、`readOnly`、および `resources.ARN` フィールドでフィルタリングして、自分にとって重要なイベントのみをログに記録するように高度なイベントセレクタを設定できます。これらのフィールドの詳細については、「」を参照してください。 AdvancedFieldSelector AWS CloudTrail APIリファレンス の「」。

AWS のエンドユーザーメッセージングソーシャル管理イベント CloudTrail

管理イベントは、 のリソースに対して実行される管理オペレーションに関する情報を提供します AWS アカウント。これらのイベントは、コントロールプレーンオペレーションとも呼ばれます。デフォルトでは、 は管理イベントを CloudTrail ログに記録します。

AWS エンドユーザーメッセージングソーシャルは、すべての AWS エンドユーザーメッセージングソーシャルコントロールプレーンオペレーションを管理イベントとしてログに記録します。 AWS エンドユーザーメッセージングソーシャルが にログ記録する AWS エンドユーザーメッセージングソーシャルコントロールプレーンオペレーションのリストについては CloudTrail、AWS 「エンドユーザーメッセージングソーシャルAPIリファレンス」を参照してください。

AWS エンドユーザーメッセージングソーシャルイベントの例

イベントは、任意の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APIオペレーション、オペレーションの日付と時刻、リクエストパラメータなどに関する情報が含まれます。 CloudTrail ログファイルはパブリックAPIコールの順序付けられたスタックトレースではないため、イベントは特定の順序で表示されません。

次の例は、 オペレーションを示す CloudTrail イベントを示しています。

```
{
        "eventVersion": "1.09",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "GR632462JDSBDSHHGS39:session",
            "arn": "arn:aws:sts::123456789101:assumed-role/Role_name/Session_name",
            "accountId": "123456789101",
            "accessKeyId": "12345678901234567890",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "GR632462JDSBDEXAMPLE",
                    "arn": "arn:aws:sts::123456789101:assumed-role/Role_name/
Session_name",
                    "accountId": "123456789101",
                    "userName": "user"
                },
                "attributes": {
                    "creationDate": "2024-10-03T17:25:08Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-10-03T17:25:23Z",
        "eventSource": "social-messaging.amazonaws.com",
        "eventName": "SendWhatsAppMessage",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "1.x.x.x",
        "userAgent": "agent",
        "requestParameters": {
            "originationPhoneNumberId": "phone-number-id-
aa01234567890123456789012345678 9",
            "metaApiVersion": "v20.0",
            "message": "Hi"
        },
        "responseElements": {
            "messageId": "message_id"
        },
        "requestID": "request_id",
        "eventID": "event_id",
        "readOnly": false,
        "resources": [{
            "accountId": "123456789101",
```

```
            "type": "AWS::SocialMessaging::PhoneNumberId",
            "ARN": "arn:aws:social-messaging:us-east-1:123456789101:phone-number-id/
phone-number-id-aa01234567890123456789012345678 9"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "123456789101",
        "eventCategory": "Data",
        "tlsDetails": {
            "clientProvidedHostHeader": "social-messaging.us-east-1.amazonaws.com"
        }
    }
```

CloudTrail レコードの内容の詳細については、「 ユーザーガイド」のCloudTrail「レコードの内容」を参照してください。 AWS CloudTrail

AWS エンドユーザーメッセージングソーシャルのベストプラクティス

このセクションでは、カスタマーエンゲージメントを向上させ、アカウントの停止を回避するのに役立ついくつかのベストプラクティスについて説明します。ただし、このセクションには法的なアドバイスは含まれていないことに注意してください。法的なアドバイスを受けるには、弁護士に相談してください。

最新の WhatsApp ベストプラクティスのリストについては、WhatsApp ビジネスメッセージングポリシー を参照してください。

トピック

Up-to-date ビジネスプロファイル

E メールアドレス、ウェブサイトアドレス、電話番号などのカスタマーサポートの連絡先情報を含む、正確で up-to-date WhatsApp ビジネスプロファイルを維持します。提供された情報が真実であり、別のビジネスを偽ったり偽ったりしないことを確認します。

許可を取得する

送信する予定のメッセージについて特定のタイプの受信を明示的に要求していない受信者には、決してメッセージを送信しないでください。次のオプトイン情報を保持します。

- オプトインプロセスでは、 経由でビジネスからメッセージまたは通話を受信することに同意していることを相手に明確に通知する必要があります WhatsApp。ビジネスの名前を明示的に記述する必要があります。

- オプトインの同意を得る方法を決定するのは、お客様の責任です。オプトインプロセスが、通信に適用されるすべての法律に準拠していることを確認します。必要な通知をすべて提供し、関連する法律で必要な許可をすべて取得します。

WhatsApp オプトイン要件の詳細については、「 のオプトインの取得」を参照してください。WhatsApp

受信者がオンラインフォームを使用してメッセージを受信するためにサインアップできる場合は、自動スクリプトが知らないユーザーをサブスクライブしないようにします。また、ユーザーが 1 回のセッションで電話番号を送信できる回数も制限します。

連絡先リストからその人を削除するなど、通信をブロック、中止、またはオプトアウトするために WhatsApp、オンかオフかにかかわらず、その人が行ったすべてのリクエストを尊重します。

日付、時刻、各オプトインリクエストおよび確認のソースが含まれる記録を保持してください。これは、顧客リストの定期的な監査を実行するのにも役立ちます。

禁止メッセージの内容

> **Important**
>
> Meta/ の使用WhatsApp
>
> - お客様による WhatsApp ビジネスソリューションの使用には、 WhatsApp サービス利用規約 、 WhatsApp ビジネスソリューション利用規約 、 WhatsApp ビジネスメッセージングポリシー 、 WhatsApp メッセージングガイドライン の利用規約、およびそれらに参照として組み込まれているその他のすべての利用規約、ポリシー、またはガイドライン (それぞれが随時更新される場合があります) が適用されます。
> - Meta または WhatsApp は、いつでも WhatsApp ビジネスソリューションの使用を禁止することができます。
> - WhatsApp ビジネスソリューションの使用に関連して、お客様は、適用される法律または規制に従って、配布の保護または制限の対象となるコンテンツ、情報、またはデータを送信しません。

WhatsApp ポリシーに違反した場合、アカウントは一定期間メッセージの送信をブロックされたり、不服申し立てを行うまでロックされたり、永続的にブロックされたりする可能性があります。Meta

は、アカウントまたはアセットがポリシーに違反したかどうかを E メールと WhatsApp ビジネスマネージャーを通じて通知します。すべての申し立ては Meta に対して行う必要があります。ポリシー違反を表示したり、Meta で申し立てを行うには、「Meta Business ヘルプセンター」の WhatsApp「ビジネスアカウントのポリシー違反の詳細を表示する」を参照してください。禁止されているメッセージコンテンツの最新のリストについては、WhatsApp「ビジネスメッセージングポリシー」を参照してください。

以下は、グローバルのすべてのメッセージタイプで禁止されているコンテンツカテゴリです。を使用してメッセージを送信する場合は WhatsApp、次のガイドラインに従ってください。

カテゴリ	例
ギャンブル	• カジノ • 宝くじ • アプリケーション/ウェブサイト
高リスク金融サービス	• 給料日ローン • 短期高利ローン • 自動車ローン • 住宅ローン • 学生ローン • 債権回収 • 在庫アラート • Cryptocurrency
債権放棄	• 債務統合 • 債務削減 • 信用回復プログラム
Get-rich-quick スキーム	• Work-from-home プログラム • リスク投資の機会 • ピラミッドまたはマルチレベルのマーケティングスキーム
違法物	• 大麻/CBD

カテゴリ	例
フィッシング/スミッシング	• ユーザーに個人情報やウェブサイトのログイン情報を開示させようと試みること。
S.H.A.F.T。	• 性別 • 憎悪 • アルコール • 銃器 • タバコ/ベイプ
サードパーティーのリード生成	• 消費者情報を購入、販売、共有する企業

顧客リストを監査する

繰り返し WhatsApp メッセージを送信する場合は、定期的に顧客リストを監査します。顧客リストを監査すると、メッセージを受信する顧客のみが受信を希望する顧客であることを確認するのに役立ちます。

リストを監査するときは、オプトインしている各顧客に、サブスクライブしていることを再確認するメッセージを送信し、サブスクライブ解除に関する情報を提供します。

エンゲージメントに基づく送信を調整する

顧客の優先順位は時間の経過とともに変わる可能性があります。顧客がメッセージを必要としなくなった場合、メッセージを完全にオプトアウトしたり、メッセージを未承諾として報告したり可能性すらあります。このため、顧客とのエンゲージメントに基づいて送信手続きを調整することは重要です。

メッセージにめったに反応しない顧客の場合、メッセージの頻度を調整する必要があります。例えば、反応の多い顧客にメッセージを毎週送信している場合、反応の少ない顧客用に別の毎月のダイジェストを作成できます。

最後に、まったく反応のない顧客を顧客リストから削除します。このステップにより、顧客がメッセージを不満に感じることがなくなります。また、コストを削減し、送信者としての評判を維持することもできます。

適切な時間に送信する

通常の日中営業時間にメッセージを送信します。夕食時または夜中にメッセージを送信すると、顧客が混乱しないようにリストからサブスクライブを解除する可能性が高くなります。顧客がすぐに応答できない場合、 WhatsApp メッセージを送信しないようにしたい場合があります。

AWS エンドユーザーメッセージングソーシャルのセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、最もセキュリティに敏感な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 とユーザーの間で責任を共有します。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ – AWS 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があります AWS クラウド。 は、安全に使用できるサービス AWS も提供します。サードパーティーの監査者は、AWS コンプライアンスプログラムコンプライアンスプログラム の一環として、当社のセキュリティの有効性を定期的にテストおよび検証。 AWS エンドユーザーメッセージングソーシャル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、AWS 「コンプライアンスプログラムによる対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウドのセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、 AWS エンドユーザーメッセージングソーシャルを使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。以下のトピックでは、セキュリティとコンプライアンスの目標を達成するために AWS エンドユーザーメッセージングソーシャルを設定する方法を示します。また、 AWS エンドユーザーメッセージングソーシャルリソースのモニタリングと保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- セキュリティに関するベストプラクティス
- AWS エンドユーザーメッセージングソーシャルのサービスにリンクされたロールの使用

AWS エンドユーザーメッセージングソーシャルのデータ保護

責任 AWS 共有モデル 、 AWS エンドユーザーメッセージングソーシャルのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービス のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「データプライバシーFAQ」を参照してください。欧州でのデータ保護の詳細については、AWS 「セキュリティブログ」のAWS 「 責任共有モデル」とGDPR「ブログ記事」を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management () を使用して個々のユーザーを設定することをお勧めしますIAM。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。1.2 が必要でTLS、1.3 TLS をお勧めします。
- で APIとユーザーアクティビティのログ記録を設定します AWS CloudTrail。証 CloudTrail 跡を使用して AWS アクティビティをキャプチャする方法については、AWS CloudTrail 「 ユーザーガイド」の CloudTrail 「証跡の操作」を参照してください。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは AWS を介して にアクセスするときに FIPS 140-3 検証済みの暗号化モジュールが必要な場合はAPI、FIPSエンドポイントを使用します。利用可能なFIPS エンドポイントの詳細については、「連邦情報処理標準 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これには、コンソール、、または API AWS CLIを使用して AWS End User Messaging Social またはその他の AWS のサービス を操

作する場合も含まれます AWS SDKs。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を に含めないことを強くお勧めします。

> **Important**
>
> WhatsApp は、安全な通信のために Signal プロトコルを使用します。ただし、 AWS エンドユーザーメッセージングソーシャルはサードパーティーであるため、これらのメッセージ WhatsApp end-to-endは暗号化されたとはみなされません。 WhatsApp データ保護の詳細については、「Data Privacy & Security and WhatsApp Encryption Overview」ホワイトペーパーを参照してください。

データ暗号化

AWS エンドユーザーメッセージングソーシャルデータは、転送中および AWS 境界内で保管中に暗号化されます。 AWS End User Messaging Social にデータを送信すると、受信時にデータが暗号化され、保存されます。 AWS End User Messaging Social からデータを取得すると、現在のセキュリティプロトコルを使用してデータが送信されます。

保管中の暗号化

AWS エンドユーザーメッセージングソーシャルは、 AWS 境界内に保存するすべてのデータを暗号化します。これには、設定データ、登録データ、および AWS エンドユーザーメッセージングソーシャルに追加するデータが含まれます。データを暗号化するために、 AWS エンドユーザーメッセージングソーシャルは、サービスがユーザーに代わって所有および維持する内部 AWS Key Management Service （ AWS KMS) キーを使用します。 AWS KMSの詳細については、『AWS Key Management Service デベロッパーガイド』を参照してください。

転送中の暗号化

AWS エンドユーザーメッセージングソーシャルは、 HTTPS および Transport Layer Security (TLS) 1.2 を使用して、クライアント、アプリケーション、および Meta と通信します。他の AWS サービスと通信するには、 AWS エンドユーザーメッセージングソーシャル は HTTPSと TLS 1.2 を使用します。さらに、コンソール、、 AWS SDKまたは を使用して AWS SMS リソースを作成および管理する場合 AWS Command Line Interface、すべての通信は HTTPSおよび 1.2 TLS を使用して保護されます。

キー管理

データを暗号化するために、 AWS エンドユーザーメッセージングソーシャルは、サービスがユーザーに代わって所有および維持する内部 AWS KMS キーを使用します。これらのキーは定期的に更新されます。End AWS User Messaging Social に保存しているデータを暗号化するために、独自のキー AWS KMS やその他のキーをプロビジョニングして使用することはできません。

ネットワーク間トラフィックのプライバシー

インターネットワークトラフィックのプライバシーとは、 AWS エンドユーザーメッセージングソーシャルとオンプレミスのクライアントとアプリケーション間、および同じ 内の AWS エンドユーザーメッセージングソーシャルと他の AWS リソース間の接続とトラフィックを保護することを意味します AWS リージョン。以下の機能とプラクティスは、 AWS エンドユーザーメッセージングソーシャルのインターネットワークトラフィックのプライバシーを保護するのに役立ちます。

AWS SMS とオンプレミスのクライアントやアプリケーションとの間のトラフィック

オンプレミスネットワーク上の AWS エンドユーザーメッセージングソーシャルとクライアントおよびアプリケーション間のプライベート接続を確立するには、 を使用できます AWS Direct Connect。これにより、標準の光ファイバーイーサネットケーブルを使用して、ネットワークを AWS Direct Connect ロケーションにリンクできます。ケーブルの一端はユーザーのルーターに接続します。もう 1 つの端は AWS Direct Connect ルーターに接続されています。詳細については、「AWS Direct Connect ユーザーガイド」の「AWS Direct Connectとは」を参照してください。

公開された を通じて AWS エンドユーザーメッセージングソーシャルへのアクセスを保護するためにAPIs、 API コールの AWS エンドユーザーメッセージングソーシャル要件に準拠することをお勧めします。 AWS エンドユーザーメッセージングソーシャルでは、クライアントが Transport Layer Security (TLS) 1.2 以降を使用する必要があります。また、クライアントは、エフェメラルディフィヘルマン (PFS) や楕円曲線ディフィエヘルマンエフェメラル () など、完全なフォワードシークレット (DHE) を持つ暗号スイートもサポートする必要がありますECDHE。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。

さらに、リクエストは、 AWS アカウントの AWS Identity and Access Management （ IAM) プリンシパルに関連付けられているアクセスキー ID と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。

AWS エンドユーザーメッセージングソーシャルのアイデンティティとアクセスの管理

AWS Identity and Access Management （ IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、 AWS エンドユーザーメッセージングソーシャルリソースの使用を認証 (サインイン) および承認 (アクセス許可を持つ) できるユーザーを制御します。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

AWS Identity and Access Management （ IAM) の使用方法は、 AWS エンドユーザーメッセージングソーシャルで行う作業によって異なります。

サービスユーザー – AWS エンドユーザーメッセージングソーシャルサービスを使用してジョブを実行する場合、管理者は必要な認証情報とアクセス許可を提供します。より多くの AWS エンドユーザーメッセージングソーシャル機能を使用して作業を行う際には、追加のアクセス許可が必要になる場合があります。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。 AWS End User Messaging Social の機能にアクセスできない場合は、「」を参照してくださいAWS エンドユーザーメッセージングソーシャルのアイデンティティとアクセスのトラブルシューティング。

サービス管理者 – 社内の AWS エンドユーザーメッセージングソーシャルリソースを担当している場合は、 AWS エンドユーザーメッセージングソーシャルへのフルアクセスが許可されている可能性があります。サービスユーザーがどの AWS エンドユーザーメッセージングソーシャル機能やリソースにアクセスする必要があるかを判断するのはお客様の仕事です。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アクセス許可を変更する必要があります。このページの情報を確認して、 の基本概念を理解しますIAM。会社が AWS エンドユーザーメッセージングソーシャルIAMで を使用する方法の詳細については、「」を参照してくださいAWS エンドユーザーメッセージングソーシャルの での仕組み IAM。

IAM 管理者 – IAM管理者の場合は、 AWS エンドユーザーメッセージングソーシャルへのアクセスを管理するポリシーの作成方法の詳細を知りたい場合があります。で使用できる AWS エンドユーザーメッセージングソーシャル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IAM、「」を参照してくださいAWS エンドユーザーメッセージングソーシャルのアイデンティティベースのポリシーの例。

アイデンティティを使用した認証

認証は、アイデンティティ認証情報 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ロールを引き受けることで、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 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と、管理者は以前に IAMロールを使用して ID フェデレーションをセットアップしていました。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、 AWS サインイン ユーザーガイドの「 へのサインイン方法 AWS アカウント」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、 はソフトウェア開発キット (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化して署名します。 AWS ツールを使用しない場合は、自分でリクエストに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「リクエストの署名 AWS API」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、 は、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用する AWS 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「多要素認証の使用」および「 ユーザーガイド」の「多要素認証の使用 (MFA) AWS」を参照してください。 IAM

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、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 ID 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してアクセスします。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザー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「ルートユーザーの認証情報を必要とするタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、 では、管理者アクセスを必要とするユーザーを含む人間のユーザーに、一時的な認証情報を使用してアクセスするために ID プロバイダーとのフェデレーション AWS のサービス の使用を要求します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリ、または ID ソースを介して提供された認証情報 AWS のサービス を使用してアクセスするすべてのユーザーからのユーザーです。フェデレーティッド ID が にアクセスすると AWS アカウント、それらはロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成したり、独自の ID ソース内のユーザーとグループのセットに接続して同期して、すべての AWS アカウント とアプリケーションで使用できます。IAM Identity Center の詳細については、AWS IAM Identity Center 「 ユーザーガイド」のIAM「Identity Center とは」を参照してください。

IAM ユーザーとグループ

IAM ユーザーとは、1 人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 ID 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持つIAMユーザーを作成する代わりに、一時的な認証情報に依存することをお勧めします。ただし、IAMユーザーとの長期的な認証情報を必要とする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ユーザーのコレクションを指定する ID 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、という名前のグループがありIAMAdmins、そのグループにIAMリソースを管理するアクセス許可を付与できます。

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 (ロールではなく) IAM ユーザーを作成するタイミング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 ID です。ユーザーと似ていますがIAM、特定の人物には関連付けられていません。IAM ロール を切り替える AWS Management Console ことで、 でロールを一時的に引き受けることができます。または AWS API オペレーションを AWS CLI 呼び出すか、カスタム を使用してロールを引き受けることができますURL。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「ロールを引き受ける方法」を参照してください。

IAM 一時的な認証情報を持つ ロールは、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ロールの詳細については、 IAM ユーザーガイドの「サードパーティー ID プロバイダーのロールの作成」を参照してください。IAM Identity Center を使用する場合は、アクセス許可セットを設定します。ID が認証された後にアクセスできる内容を制御するために、IAMIdentity Center はアクセス許可セットを のロールに関連付けますIAM。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ユーザーアクセス許可 – IAM ユーザーまたはロールは、特定のタスクに対して異なるアクセス許可を一時的に引き受けるIAMロールを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、別のアカウントの誰か (信頼できるプリンシパル) が自分のアカウントのリソースにアクセスすることを許可できます。クロスアカウントアクセスを許可する主な方法は、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、 (プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。

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「 のクロスアカウントリソースアクセスIAM」を参照してください。

- クロスサービスアクセス — 他の の機能 AWS のサービス を使用するものもあります AWS のサービス。例えば、サービスで呼び出しを行うと、そのサービスが Amazon でアプリケーションを実行EC2したりAmazon S3にオブジェクトを保存したりするのが一般的です。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と AWS、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と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストを使用します。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権限が必要です。FAS リクエストを行う際のポリシーの詳細については、「アクセスセッションの転送」を参照してください。
  - サービスロール – サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受けるIAMロールです。IAM 管理者は、 内からサービスロールを作成、変更、削除できますIAM。詳細については、IAM「 ユーザーガイド」の「 にアクセス許可を委任するロールの作成 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 – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、 サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示することはできますが、編集することはできません。
- Amazon で実行されているアプリケーション EC2 – 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インスタンス内にアクセスキーを保存するよりも望ましいです。 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 ロールが含まれており、EC2インスタンスで実行されているプログラムが一時的な認証情報を取得できるようにします。詳細については、IAM「 ユーザーガイド」のIAM「ロールを使用して Amazon EC2インスタンスで実行されているアプリケーションにアクセス許可を付与する」を参照してください。

IAM ロールとIAMユーザーのどちらを使用するかについては、IAM「 ユーザーガイド」の「(ユーザーではなく) IAMロールを作成するタイミング」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には、ポリシー AWS を作成し、 AWS ID またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義するオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーはJSONドキュメント AWS として 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、「 ユーザーガイド」のJSON「ポリシーの概要」を参照してください。 IAM

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

デフォルトでは、ユーザーやロールに権限はありません。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するには、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行に使用する方法に関係なく、アクションのアクセス許可を定義します。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 からロール情報を取得できますAPI。

アイデンティティベースのポリシー

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできるJSONアクセス許可ポリシードキュメントです。これらのポリシーは、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。ID 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。マネージドポリシーは、 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選択」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、リソースにアタッチする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の例としては、IAMロール信頼ポリシー と Amazon S3 バケットポリシー があります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、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IAMでは、 から AWS 管理ポリシーを使用することはできません。

アクセスコントロールリスト (ACLs)

アクセスコントロールリスト (ACLs) 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アクセス許可を持つかを制御します。ACLs 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されません。

Amazon S3、および Amazon VPCは AWS WAF、 をサポートするサービスの例ですACLs。の詳細についてはACLs、「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) 概要」を参照してください。

その他のポリシータイプ

AWS は、追加の低頻度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がIAMエンティティ (IAMユーザーまたはロール) に付与できる最大アクセス許可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) の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、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ためのサービス AWS アカウント 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 (SCPs) をアカウントの一部またはすべてに適用できます。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SCPを制限します AWS アカウントのルートユーザー。Organizations と の詳細についてはSCPs、AWS Organizations 「 ユーザーガイド」の「サービスコントロールポリシー」を参照してください。

- 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、「 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。 IAM

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。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、IAM「 ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

AWS エンドユーザーメッセージングソーシャルの での仕組み IAM

IAM を使用して AWS エンドユーザーメッセージングソーシャルへのアクセスを管理する前に、AWS エンドユーザーメッセージングソーシャルで使用できるIAM機能について説明します。

IAM AWS エンドユーザーメッセージングソーシャルで使用できる機能

IAM 機能	AWS エンドユーザーメッセージングソーシャルサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	Yes
ポリシー条件キー	可能

IAM 機能	AWS エンドユーザーメッセージングソーシャルサポート
ACLs	不可
ABAC (ポリシーのタグ)	部分的
一時的な認証情報	あり
プリンシパル権限	あり
サービスロール	あり
サービスリンクロール	可能

End AWS User Messaging Social およびその他の AWS のサービスがほとんどのIAM機能でどのように機能するかの概要を確認するには、 IAM ユーザーガイドのAWS 「 で機能する のサービスIAM」を参照してください。

AWS エンドユーザーメッセージングソーシャルのアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできるJSONアクセス許可ポリシードキュメントです。これらのポリシーは、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。ID 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。

IAM ID ベースのポリシーでは、許可または拒否されたアクションとリソース、およびアクションが許可または拒否される条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素については、IAM「 ユーザーガイド」のIAMJSON「ポリシー要素リファレンス」を参照してください。

AWS エンドユーザーメッセージングソーシャルのアイデンティティベースのポリシーの例

AWS エンドユーザーメッセージングソーシャルアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS エンドユーザーメッセージングソーシャルのアイデンティティベースのポリシーの例。

AWS エンドユーザーメッセージングソーシャル内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースにアタッチする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の例としては、IAMロール信頼ポリシー と Amazon S3 バケットポリシー があります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、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。

クロスアカウントアクセスを有効にするには、リソースベースのポリシーのプリンシパルとして、別のアカウントのアカウントまたはIAMエンティティ全体を指定できます。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる にある場合 AWS アカウント、信頼されたアカウントのIAM管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、IAM「 ユーザーガイド」の「 のクロスアカウントリソースアクセスIAM」を参照してください。

AWS エンドユーザーメッセージングソーシャルのポリシーアクション

ポリシーアクションのサポート: あり

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

JSON ポリシーの `Action`要素は、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を記述します。ポリシーアクションは通常、関連付けられた AWS APIオペレーションと同じ名前です。一致するAPIオペレーションがないアクセス許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

AWS エンドユーザーメッセージングソーシャルアクションのリストを確認するには、「サービス認証リファレンス」のAWS「エンドユーザーメッセージングソーシャルで定義されるアクション」を参照してください。

AWS End User Messaging Social のポリシーアクションは、アクションの前に次のプレフィックスを使用します。

```
social-messaging
```

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

```
"Action": [
      "social-messaging:action1",
      "social-messaging:action2"
         ]
```

AWS エンドユーザーメッセージングソーシャルアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS エンドユーザーメッセージングソーシャルのアイデンティティベースのポリシーの例。

AWS エンドユーザーメッセージングソーシャルのポリシーリソース

ポリシーリソースのサポート: あり

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

Resource JSON ポリシー要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

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

AWS エンドユーザーメッセージングソーシャルリソースタイプとその のリストを確認するには ARNs、「サービス認証リファレンス」のAWS 「エンドユーザーメッセージングソーシャルで定義されるリソース」を参照してください。各リソースARNの を指定できるアクションについては、AWS 「エンドユーザーメッセージングソーシャルで定義されるアクション」を参照してください。

AWS エンドユーザーメッセージングソーシャルアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS エンドユーザーメッセージングソーシャルのアイデンティティベースのポリシーの例。

AWS エンドユーザーメッセージングソーシャルのポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

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

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば、IAMユーザー名でタグ付けされている場合にのみ、リソースにアクセスするアクセス許可をIAMユーザーに付与できます。詳細については、「 ユーザーガイド」のIAM「ポリシー要素: 変数とタグ」を参照してください。 IAM

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべての AWS グローバル条件キーを確認するには、 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。 IAM

AWS エンドユーザーメッセージングソーシャルの条件キーのリストを確認するには、「サービス認証リファレンス」の AWS 「エンドユーザーメッセージングソーシャルの条件キー」を参照してくだ

さい。条件キーを使用できるアクションとリソースについては、AWS「エンドユーザーメッセージングソーシャルで定義されるアクション」を参照してください。

AWS エンドユーザーメッセージングソーシャルアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS エンドユーザーメッセージングソーシャルのアイデンティティベースのポリシーの例。

ACLs AWS エンドユーザーメッセージングソーシャル

をサポートACLs： なし

アクセスコントロールリスト (ACLs) 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アクセス許可を持つかを制御します。ACLs 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されません。

ABAC AWS エンドユーザーメッセージングソーシャルを使用する

サポート ABAC (ポリシーのタグ): 部分的

属性ベースのアクセスコントロール (ABAC) は、属性に基づいてアクセス許可を定義する認証戦略です。では AWS、これらの属性はタグ と呼ばれます。タグは、IAMエンティティ (ユーザーまたはロール) と多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、 の最初のステップですABAC。次に、プリンシパルのタグがアクセスしようとしているリソースのタグと一致するときに、オペレーションを許可するABACポリシーを設計します。

ABAC は、急速に成長している環境や、ポリシー管理が面倒になる状況に役立ちます。

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

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

の詳細についてはABAC、 IAM ユーザーガイドの「 とはABAC」を参照してください。を設定する手順を含むチュートリアルを表示するにはABAC、 IAM ユーザーガイドの「属性ベースのアクセスコントロールを使用する (ABAC) 」を参照してください。

AWS エンドユーザーメッセージングソーシャルでの一時的な認証情報の使用

一時的な認証情報のサポート: あり

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報 AWS のサービス を使用する方法などの詳細については、 IAM ユーザーガイドの AWS のサービス を使用するIAM方法を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社のシングルサインオン (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えの詳細については、IAM「 ユーザーガイド」の「ロールへの切り替え (コンソール) 」を参照してください。

AWS CLI または を使用して、一時的な認証情報を手動で作成できます AWS API。その後、これらの一時的な認証情報を使用して にアクセスできます AWS。長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成 AWS することをお勧めします。詳細については、「」の「一時的なセキュリティ認証情報IAM」を参照してください。

AWS エンドユーザーメッセージングソーシャルのクロスサービスプリンシパルアクセス許可

転送アクセスセッションをサポート (FAS): はい

ユーザーIAMまたはロールを使用して でアクションを実行すると AWS、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権限が必要です。FAS リクエストを行う際のポリシーの詳細については、「アクセスセッションの転送」を参照してください。

AWS エンドユーザーメッセージングソーシャルのサービスロール

サービスロールのサポート: あり

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

> **Warning**
>
> サービスロールのアクセス許可を変更すると、 AWS エンドユーザーメッセージングソーシャル機能が損なわれる可能性があります。 AWS End User Messaging Social が指示する場合にのみ、サービスロールを編集します。

AWS エンドユーザーメッセージングソーシャルのサービスにリンクされたロール

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、 サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示することはできますが、編集することはできません。

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

AWS エンドユーザーメッセージングソーシャルのアイデンティティベースのポリシーの例

デフォルトでは、ユーザーとロールには、 AWS エンドユーザーメッセージングソーシャルリソースを作成または変更するアクセス許可がありません。また、、 AWS Command Line Interface （ AWS CLI ）AWS Management Console、または を使用してタスクを実行することはできません AWS API。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するには、IAM 管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

これらのポリシードキュメント例を使用して IAM ID ベースのJSON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。

ARNs 各リソースタイプの の形式など、 AWS エンドユーザーメッセージングソーシャルで定義されるアクションとリソースタイプの詳細については、「サービス認証リファレンス」のAWS 「エンドユーザーメッセージングソーシャルのアクション、リソース、および条件キー」を参照してください。

トピック

- ポリシーのベストプラクティス
- AWS エンドユーザーメッセージングソーシャルコンソールの使用
- 自分の権限の表示をユーザーに許可する

ポリシーのベストプラクティス

ID ベースのポリシーは、アカウント内の AWS エンドユーザーメッセージングソーシャルリソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションを実行すると、AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS マネージドポリシーを開始し、最小権限のアクセス許可に移行 – ユーザーとワークロードへのアクセス許可の付与を開始するには、多くの一般的なユースケースのアクセス許可を付与するAWS マネージドポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、IAM「 ユーザーガイド」の「 管理AWS ポリシー」または「 ジョブ機能の 管理ポリシー」を参照してください。 AWS
- 最小権限のアクセス許可を適用する - IAMポリシーでアクセス許可を設定する場合、タスクの実行に必要なアクセス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 を使用してアクセス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「 のポリシーとアクセス許可IAM」を参照してください。
- IAM ポリシーの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、アクションと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 を使用して送信する必要があることを指定できますSSL。また、 などの特定の を通じてサービスアクションが使用されている場合 AWS のサービス、 条件を使用してサービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、IAM「 ユーザーガイド」のIAMJSON「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、安全で機能的なアクセス許可を確保する – IAM Access Analyzer は、ポリシーがポリシー言語 (JSON) とIAMベストプラクティスに準拠するように、新規および既存のIAMポリシーを検証します。IAM Access Analyzer には、安全で機能的なポリシーの作成に役立つ 100 を超えるポリシーチェックと実用的なレコメンデーションが用意されています。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。

- 多要素認証が必要 (MFA) – 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、 をオンにMFAしてセキュリティを強化します。API オペレーションが呼び出されるMFAタイミングを要求するには、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。

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「 のセキュリティのベストプラクティスIAM」を参照してください。 IAM

AWS エンドユーザーメッセージングソーシャルコンソールの使用

AWS エンドユーザーメッセージングソーシャルコンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の AWS エンドユーザーメッセージングソーシャルリソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または 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 AWS API。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を許可します。

ユーザーとロールが引き続き AWS エンドユーザーメッセージングソーシャルコンソールを使用できるようにするには、 AWS エンドユーザーメッセージングソーシャル*ConsoleAccess*または*ReadOnly* AWS マネージドポリシーをエンティティにアタッチします。詳細については、「 ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。 IAM

自分の権限の表示をユーザーに許可する

この例では、IAMユーザーがユーザー ID にアタッチされているインラインポリシーとマネージドポリシーを表示できるようにするポリシーを作成する方法を示します。このポリシーには、コンソールで、または AWS CLI または 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 AWS API。

```
{
    "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": "*"
        }
    ]
}
```

AWSAWS エンドユーザーメッセージングソーシャルの マネージドポリシー

ユーザー、グループ、ロールにアクセス許可を追加するには、自分でポリシーを記述するよりも、AWS 管理ポリシーを使用する方が簡単です。必要なアクセス許可のみをチームに提供するIAMカスタマー管理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ターゲット範囲に含めており、 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、「 ユーザーガイド」のAWS 「 管理ポリシー」を参照してください。 IAM

AWS サービスは、 AWS マネージドポリシーを維持および更新します。 AWS マネージドポリシーのアクセス許可は変更できません。サービスでは、新しい機能を利用できるようにするために、

AWS マネージドポリシーに権限が追加されることがあります。この種類の更新は、ポリシーがアタッチされている、すべてのアイデンティティ (ユーザー、グループおよびロール) に影響を与えます。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスが AWS マネージドポリシーを更新する可能性が最も高くなります。サービスは AWS 管理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損なわ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ジョブ関数のマネージドポリシー AWS をサポートしています。例えば、 ReadOnlyAccess AWS マネージドポリシーは、すべての AWS サービスとリソースへの読み取り専用アクセスを提供します。サービスが新機能を起動すると、 は新しいオペレーションとリソースの読み取り専用アクセス許可 AWS を追加します。ジョブ関数ポリシーのリストと説明については、「 ユーザーガイド」のAWS 「ジョブ関数の管理ポリシー」を参照してください。 IAM

AWSAWS マネージドポリシーへのエンドユーザーメッセージングソーシャルの更新

このサービスがこれらの変更の追跡を開始してからの AWS エンドユーザーメッセージングソーシャルの AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動アラートについては、 AWS エンドユーザーメッセージングのソーシャルドキュメント履歴ページのRSSフィードにサブスクライブします。

変更	説明	日付
AWS エンドユーザーメッセージングソーシャルが変更の追跡を開始しました	AWS エンドユーザーメッセージングソーシャルは、その AWS 管理ポリシーの変更の追跡を開始しました。	2024 年 9 月 26 日

AWS エンドユーザーメッセージングソーシャルのアイデンティティとアクセスのトラブルシューティング

以下の情報は、 AWS エンドユーザーメッセージングソーシャル および の使用時に発生する可能性のある一般的な問題を診断して修正するのに役立ちますIAM。

トピック

AWS エンドユーザーメッセージングソーシャルでアクションを実行する権限がありません

「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、mateojacksonIAMユーザーがコンソールを使用して架空の*my-example-widget*リソースの詳細を表示しようとしても、架空のsocial-messaging:*GetWidget*アクセス許可がない場合に発生します。

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

この場合、social-messaging:*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、 AWS エンドユーザーメッセージングソーシャルにロールを渡すことができるようにポリシーを更新する必要があります。

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

次のエラー例は、 という名前のIAMユーザーがコンソールを使用して AWS End User Messaging Social marymajor でアクションを実行しようとすると発生します。ただし、このアクションをサー

ビスが実行するには、サービスロールから付与された権限が必要です。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。

自分の外部のユーザーに AWS エンドユーザーメッセージングソーシャルリソース AWS アカウント 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 (ACLs) をサポートするサービスでは、これらのポリシーを使用して、リソースへのアクセスをユーザーに許可できます。

詳細については、以下を参照してください。

- AWS エンドユーザーメッセージングソーシャルがこれらの機能をサポートしているかどうかについては、「」を参照してくださいAWS エンドユーザーメッセージングソーシャルの での仕組み IAM。
- 所有 AWS アカウント している 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。
- サードパーティー にリソースへのアクセスを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「サードパーティーが所有する へのアクセスを提供する AWS アカウント」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を提供する (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にロールとリソースベースのポリシーを使用する違いについては、IAM ユーザーガイドの「 のクロスアカウントリソースアクセスIAM」を参照してください。

AWS エンドユーザーメッセージングソーシャルのコンプライアンス検証

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、AWS のサービス「コンプライアンスプログラムによるスコープ」の」の「」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することができます AWS Artifact。詳細については、「」の AWS Artifact」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、データの機密性、会社のコンプライアンス目的、および適用される法律と規制によって決まります。 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。
- Amazon Web Services HIPAA のセキュリティとコンプライアンスのためのアーキテクチャ – このホワイトペーパーでは、企業が AWS を使用して HIPAAの対象となる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**
>
> すべての AWS のサービス がHIPAA対象となるわけではありません。詳細については、HIPAA「対象サービスリファレンス」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、お客様の業界とロケーション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 ()、国際標準化機構 (ISO) などPCI) 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。
- AWS Config 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、リソース設定が内部プラクティス、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 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 を検出できます。 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出要件を満たすことでDSS、 PCI などのさまざまなコンプライアンス要件に対応するのに役立ちます。
- 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、リスクと規制や業界標準へのコンプライアンスの管理を簡素化できます。

AWS エンドユーザーメッセージングソーシャルの回復力

AWS グローバルインフラストラクチャは、 AWS リージョン および アベイラビリティーゾーンを中心に構築されています。複数の物理的に分離および分離されたアベイラビリティーゾーン AWS リージョン を提供し、低レイテンシー、高スループット、および冗長性の高いネットワークで接続されます。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 およびアベイラビリティーゾーンの詳細については、AWS 「グローバルインフラストラクチャ」を参照してください。

AWS グローバルインフラストラクチャに加えて、 AWS End User Messaging Social には、データの耐障害性とバックアップのニーズをサポートするのに役立つ機能がいくつか用意されています。

AWS エンドユーザーメッセージングソーシャルのインフラストラクチャセキュリティ

マネージドサービスである AWS エンドユーザーメッセージングソーシャルは、Amazon Web Services: セキュリティプロセスの概要ホワイトペーパーに記載されている AWS グローバルネットワークセキュリティ手順によって保護されています。

AWS 公開されたAPI呼び出しを使用して、ネットワーク経由で AWS エンドユーザーメッセージングソーシャルにアクセスします。クライアントは Transport Layer Security (TLS) 1.0 以降をサポートする必要があります。1.2 TLS 以降をお勧めします。また、クライアントは、 (エフェメラルディフィーヘルマンPFS) や DHE (エリプティックカーブエフェメラルディフィーヘルマン) など、完全なフォワードシークレット ECDHE () を持つ暗号スイートもサポートする必要があります。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

さらに、リクエストは、アクセスキー ID とプリンシIAM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、テンポラリ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。

サービス間の混乱した代理の防止

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

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

混乱した代理問題から保護する最も効果的な方法は、リソースがいっぱいARNになった `aws:SourceArn` グローバル条件コンテキストキーを使用することです。リソースARNの完全版がわからない場合や、複数のリソースを指定する場合は、 の不明な部分に対してワイルドカード文字 (*) を含む`aws:SourceArn`グローバルコンテキスト条件キーを使用しますARN。例えば、`arn:aws:social-messaging:*:`*`123456789012`*`:*` と指定します。

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

`aws:SourceArn` の値は ResourceDescription である必要があります。

次の例は、ソーシャルメッセージングで aws:SourceArnおよび aws:SourceAccount グローバル条件コンテキストキーを使用して、混乱した代理問題を防ぐ方法を示しています。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "social-messaging.amazonaws.com"
    },
    "Action": "social-messaging:ActionName",
    "Resource": [
      "arn:aws:social-messaging:::ResourceName/*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:social-messaging:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

セキュリティに関するベストプラクティス

AWS エンドユーザーメッセージングソーシャルには、独自のセキュリティポリシーを開発および実装する際に考慮すべきセキュリティ機能が多数用意されています。以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションを説明するものではありません。これらのベストプラクティスはお客様の環境に必ずしも適切または十分でない可能性があるので、処方箋ではなく、あくまで有用な考慮事項とお考えください。

- 自分自身を含む AWS SMS リソースを管理するユーザーごとに、個々のユーザーを作成します。AWS SMS リソースの管理に AWS ルート認証情報を使用しないでください。
- それぞれの職務の実行に最低限必要になる一連のアクセス許可を各ユーザーに付与します。
- IAM グループを使用して、複数のユーザーのアクセス許可を効果的に管理します。
- IAM 認証情報のローテーションを定期的に行います。

AWS エンドユーザーメッセージングソーシャルのサービスにリンクされたロールの使用

AWS エンドユーザーメッセージングソーシャルは AWS Identity and Access Management 、 (IAM) サービスにリンクされたロール を使用します。サービスにリンクされたロールは、 AWS エンドユーザーメッセージングソーシャルに直接リンクされる一意のタイプのIAMロールです。サービスにリンクされたロールは、 AWS エンドユーザーメッセージングソーシャルによって事前定義されており、ユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がないため、 AWS エンドユーザーメッセージングソーシャルの設定が容易になります。 AWS エンドユーザーメッセージングソーシャルは、サービスにリンクされたロールのアクセス許可を定義し、特に定義されていない限り、 AWS エンドユーザーメッセージングソーシャル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、そのアクセス許可ポリシーを他のIAMエンティティにアタッチすることはできません。

サービスリンクロールは、まずその関連リソースを削除しなければ削除できません。これにより、リソースへのアクセス許可を誤って削除できないため、 AWS エンドユーザーメッセージングソーシャルリソースが保護されます。

サービスにリンクされたロールをサポートする他のサービスの詳細については、AWS 「 と連携するIAMサービス」を参照してください。また、「サービスにリンクされたロール」列で「はい」のサービスを探します。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、[Yes] (はい) リンクを選択します。

AWS エンドユーザーメッセージングソーシャルのサービスにリンクされたロールのアクセス許可

AWS エンドユーザーメッセージングソーシャルは、 AWSServiceRoleForSocialMessaging という名前のサービスにリンクされたロールを使用します。メトリクスを発行し、ソーシャルメッセージ送信に関するインサイトを提供します。

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

- `social-messaging.amazonaws.com`

という名前のロールアクセス許可ポリシー AWSSocialMessagingServiceRolePolicy により、 AWS エンドユーザーメッセージングソーシャルは、指定されたリソースに対して次のアクションを実行できます。

- アクション: `all AWS resources in the AWS/SocialMessaging namespace.` 上で `"cloudwatch:PutMetricData"`

ユーザー、グループ、ロールなどがサービスにリンクされたロールを作成、編集、削除できるようにするには、アクセス権限を設定する必要があります。詳細については、「 ユーザーガイド」の「サービスにリンクされたロールのアクセス許可」を参照してください。 IAM

ポリシーの更新については、「」を参照してくださいAWSAWS マネージドポリシーへのエンドユーザーメッセージングソーシャルの更新。

AWS エンドユーザーメッセージングソーシャルのサービスにリンクされたロールの作成

IAM コンソールを使用して、 AWSEndUserMessagingSocial- Metrics ユースケースを使用してサービスにリンクされたロールを作成できます。 AWS CLI または で AWS API、サービス名を使用して`social-messaging.amazonaws.com`サービスにリンクされたロールを作成します。詳細については、「 ユーザーガイド」の「サービスにリンクされたロールの作成」を参照してください。 IAM このサービスリンクロールを削除しても、同じ方法でロールを再作成できます。

AWS エンドユーザーメッセージングソーシャルのサービスにリンクされたロールの編集

AWS エンドユーザーメッセージングソーシャルでは、 AWSServiceRoleForSocialMessaging サービスにリンクされたロールを編集することはできません。サービスリンクロールを作成した後は、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、 を使用してロールの説明を編集できますIAM。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。

AWS エンドユーザーメッセージングソーシャルのサービスにリンクされたロールの削除

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

ティティを排除できます。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースの削除時に AWS エンドユーザーメッセージングソーシャルサービスがロールを使用している場合、削除が失敗する可能性があります。失敗した場合は、数分待ってから操作を再試行してください。

で使用される AWS エンドユーザーメッセージングソーシャルリソースを削除するには AWSServiceRoleForSocialMessaging

1. を呼び出し`list-linked-whatsapp-business-accounts`APIて、使用しているリソースを確認します。
2. リンクされた Whats App Business アカウントごとに、 `disassociate-whatsapp-business-account`APIを呼び出して SocialMessaging 、サービスからリソースを削除します。
3. `list-linked-whatsapp-business-accounts` API を再度呼び出して、リソースが返されないことを確認します。

を使用してサービスにリンクされたロールを手動で削除するには IAM

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

AWS エンドユーザーメッセージングソーシャルサービスにリンクされたロールでサポートされているリージョン

AWS エンドユーザーメッセージングソーシャルは、サービスが利用可能なすべてのリージョンでサービスにリンクされたロールの使用をサポートしています。詳細については、「AWS リージョンとエンドポイント」を参照してください。

AWS エンドユーザーメッセージングソーシャルのクォータ

AWS アカウントには、AWSサービスごとに、以前は制限と呼ばれていたデフォルトのクォータがあります。特に明記されていない限り、クォータは地域固有です。一部のクォータについては引き上げをリクエストできますが、その他のクォータについては引き上げることはできません。

AWS エンドユーザーメッセージングソーシャルのクォータを表示するには、Service Quotas コンソール を開きます。ナビゲーションペインで、AWSサービスを選択し、AWS エンドユーザーメッセージングソーシャル を選択します。

クォータの引き上げをリクエストするには、Service Quotas ユーザーガイド の「クォータ引き上げリクエスト」を参照してください。Service Quotas でクォータがまだ利用できない場合は、[上限引き上げ] フォームを使用してください。

AWS アカウントには、 AWS エンドユーザーメッセージングソーシャルに関連する以下のクォータがあります。

リソース	デフォルト
WhatsApp ビジネスアカウント (WABA)	リージョンあたり 25

AWS エンドユーザーメッセージングソーシャルは、 APIから AWS エンドユーザーメッセージングソーシャルに実行できるリクエストの数を制限するクォータを実装します AWS アカウント。

操作	Rate
SendWhatsAppMessage	1,000
PostWhatsAppMessageMedia	100
GetWhatsAppMessageMedia	100
DeleteWhatsAppMessageMedia	100
DisassociateWhatsAppBusinessAccount	10
ListWhatsAppBusinessAccount	10

操作	Rate
TagResource	10
UntagResourceRate	10
ListTagsForResourceRate	10

AWS エンドユーザーメッセージングソーシャルユーザーガイドのドキュメント履歴

次の表は、 AWS エンドユーザーメッセージングソーシャルのドキュメントリリースを示しています。

変更	説明	日付
初回リリース	AWS エンドユーザーメッセージングソーシャルユーザーガイドの初回リリース	2024 年 10 月 10 日

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