aws

管理ガイド AWS Wickr



Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Wickr: 管理ガイド

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

AWS Wickr とは?	. 1
Wickr の特徴	. 1
リージョナルな可用性	. 3
Wickr へのアクセス	. 3
料金	. 3
Wickr エンドユーザ向けドキュメント	. 3
設定	. 4
にサインアップする AWS	. 4
IAM ユーザーの作成	. 4
次のステップ	. 5
入門	. 6
前提条件	. 6
ステップ1: ネットワークの構築	. 6
ステップ 2: ネットワークの構成	. 7
ステップ 3: ユーザーを作成して招待する	. 8
次のステップ	10
ネットワークの管理	11
ネットワークの詳細	11
ネットワークの詳細を表示する	11
ネットワーク名の編集	12
ネットワークの削除	12
セキュリティグループ	13
セキュリティグループの表示	13
セキュリティグループを作成する	14
セキュリティグループを編集する	14
セキュリティグループを削除する	17
SSO 設定	18
SSO の詳細の表示	18
SSO の設定	18
トークン更新の猶予期間	27
ネットワークタグ	27
ネットワークタグの管理	27
ネットワークタグを追加する	28
ネットワークタグを編集する	28

ネットワークタグを削除する	
受信の読み取り	29
ネットワークプランの管理	30
プレミアム無料トライアルの制限	30
データ保持	31
データ保持の表示	31
データ保持を設定する	32
ログの取得	43
データ保持指標とイベント	44
ATAK とは	49
ATAK を有効にする	50
ATAK に関する追加情報	51
インストールとペアリング	51
ペア解除	53
ダイヤル発信と着信	53
ファイルの送信	53
安全な音声メッセージを送信する	54
ピンホイール	56
ナビゲーション	58
許可するポートとドメインのリスト	59
リージョン別の許可リストのドメインとアドレス	59
GovCloud	69
ファイルプレビュー	71
ユーザーの管理	73
チームディレクトリ	73
ユーザーを表示する	73
ユーザーを招待する	74
ユーザーの編集	74
ユーザーの削除	75
ユーザーの一括削除	75
ユーザーの一括停止	77
ゲストユーザー	
ゲストユーザーを有効または無効にする	
ゲストユーザー数の表示	79
毎月の使用状況の表示	80
ゲストユーザーの表示	80

ゲストユーザーをブロックする	81
セキュリティ	
データ保護	83
ID とアクセス管理	84
対象者	
アイデンティティを使用した認証	85
ポリシーを使用したアクセスの管理	
AWS Wickr のマネージドポリシー	
AWS Wickr と IAM の連携方法	
アイデンティティベースのポリシーの例	
トラブルシューティング	102
コンプライアンス検証	103
耐障害性	103
インフラストラクチャセキュリティ	104
設定と脆弱性の分析	104
セキュリティに関するベストプラクティス	104
モニタリング	105
CloudTrail ログ	105
CloudTrailのWickr情報	105
Wickrのログファイルエントリーを理解します。	106
分析ダッシュボード	113
ドキュメント履歴	116
リリースノート	121
2025 年 5 月	121
2025 年 3 月	121
2024 年 10 月	121
2024 年 9 月	121
2024 年 8 月	121
2024 年 6 月	122
2024 年 4 月	122
2024 年 3 月	122
2024 年 2 月	122
2023 年 11 月	122
2023 年 10 月	123
2023 年 9 月	123
2023 年 8 月	123

7月	123
5月	124
3 月	124
2月	124
1月	124
c	xxv

AWS Wickr とは?

AWS Wickr は、エンドツーエンドの暗号化サービスです。これにより組織や政府機関は、1 対 1 お よびグループでのメッセージング、音声およびビデオ通話、ファイル共有、画面共有、その他を通じ ての通信を安全に行えるようになります。Wickr は、コンシューマーグレードのメッセージングアプ リに関連するデータ保持義務を顧客が克服し、コラボレーションを安全に促進できるよう支援しま す。高度なセキュリティと管理制御により、組織は法的要件や規制要件を満たし、データセキュリ ティの課題に対応するカスタムソリューションを構築できます。

情報は、保存や監査の目的で、カスタマーが管理するプライベートなデータストアに記録できます。 ユーザーは、権限の設定、エフェメラルメッセージングオプションの設定、セキュリティグループ の定義など、データを包括的に管理できます。Wickr は、アクティブディレクトリ (AD)、OpenID Connect (OIDC) によるシングルサインオン (SSO) などの追加サービスと統合されます。を使用して Wickr ネットワークをすばやく作成および管理し AWS Management Console、Wickr ボットを使用 してワークフローを安全に自動化できます。開始するには、「<u>AWS Wickr 用のセットアップ</u>」を参 照してください。

トピック

- Wickr の特徴
- リージョナルな可用性
- Wickr へのアクセス
- 料金
- Wickr エンドユーザ向けドキュメント

Wickr の特徴

セキュリティとプライバシーの強化

Wickr は、すべての機能に 256 ビット高度暗号化標準 (AES) のエンドツーエンド暗号化を使用して います。通信はユーザーデバイス上でローカルに暗号化され、送信者と受信者以外への転送中は解読 できません。すべてのメッセージ、呼び出し、ファイルは新しいランダムキーで暗号化され、意図し た受信者以外 (偶数ではない AWS) は復号できません。機密データや規制対象データの共有、法的問 題や人事に関する議論、戦術的な軍事作戦の実施など、セキュリティとプライバシーが最優先される 場合、カスタマーは Wickr を使用して通信します。

データ保持

柔軟な管理機能は、機密情報を保護するだけでなく、コンプライアンス義務、法的保持、監査目的で 必要に応じてデータを保持するように設計されています。メッセージとファイルは、カスタマーが管 理する安全なデータストアにアーカイブできます。

柔軟なアクセス

ユーザーはマルチデバイス(モバイル、デスクトップ)にアクセスでき、非接続通信や帯域外通信な どの低帯域幅環境でも機能することができます。

管理コントロール

ユーザーは、権限の設定、責任がありエフェメラルメッセージングオプションの設定、セキュリティ グループの定義など、データを包括的に管理できます。

強力なインテグレーションとボット

Wickr は、アクティブディレクトリ、OpenID Connect (OIDC) によるシングルサインオン (SSO) な どの追加サービスと統合されます。お客様は、 を通じて Wickr ネットワークをすばやく作成および 管理し AWS Management Console、Wickr Bots を使用してワークフローを安全に自動化できます。

Wickr が提供するコラボレーションの内訳は次のとおりです。

- 1対1メッセージとグループメッセージング:最大 500人のメンバーがいるルームで、チームと安全にチャットできます
- 音声通話とビデオ通話: 最大 70 人で電話会議を開催できます
- 画面共有とブロードキャスト: 最大 500 人の参加者が参加できます
- ファイル共有と保存:最大5GBまでファイルを転送でき、ストレージ容量は無制限です
- ・エフェメラル: 有効期限とBurn-on-Read (BOR) タイマーの制御
- グローバルフェデレーション: ネットワーク外の Wickr ユーザーと接続する

Note

AWS GovCloud (米国西部) の Wickr ネットワークは、 AWS GovCloud (米国西部) の他の Wickr ネットワークとのみフェデレーションできます。

リージョナルな可用性

Wickr は、米国東部 (バージニア北部)、アジアパシフィック (マレーシア)、アジアパシフィッ ク (シンガポール)、アジアパシフィック (シドニー)、アジアパシフィック (東京)、カナダ (中 部)、欧州 (フランクフルト)、欧州 (ロンドン)、欧州 (ストックホルム)、欧州 (チューリッヒ) で利用できます AWS リージョン。Wickr は AWS GovCloud (米国西部) リージョンでも利用できま す。各リージョンには複数のアベイラビリティーゾーンがあり、物理的に分離されていますが、プラ イベート、低レイテンシー、高帯域幅、冗長ネットワーク接続で接続されています。これらのアベイ ラビリティーゾーンは、可用性の向上、耐障害性、レイテンシーの最小化に使用されます。

詳細については AWS リージョン、「」の<u>AWS リージョン 「アカウントで使用できる を指定する</u>」 を参照してくださいAWS 全般のリファレンス。各リージョンで使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。

Wickr へのアクセス

管理者は <u>https://console.aws.amazon.com/wickr/</u>://www.ital-in AWS Management Console -re-re-dre-d-d-re-d-re-d-re-d-d- Wickr を使い始める前に、<u>AWS Wickr 用のセットアップ</u> および <u>AWS Wickr</u> の使用開始 ガイドを完成させる必要があります。

Note

Wickr サービスには、アプリケーションプログラミングインターフェイス (API) はありません。

エンドユーザーは Wickr クライアントを通じて Wickr にアクセスします。詳細は、「<u>AWS Wickr</u> ユーザーガイド」を参照してください。

料金

Wickr は、個人、小規模チーム、大企業向けにさまざまなプランで利用できます。詳細については、 「AWS Wickr の料金」を参照してください。

Wickr エンドユーザ向けドキュメント

Wickr クライアントのエンドユーザーで、そのドキュメントにアクセスする必要がある場合は、 「AWS Wickr ユーザーガイド」を参照してください。

AWS Wickr 用のセットアップ

新規の AWS お客様は、AWS Wickr の使用を開始する前に、このページに記載されているセット アップの前提条件を完了してください。これらのセットアップ手順では、 AWS Identity and Access Management (IAM) サービスを使用します。IAM の詳細については、「<u>IAM ユーザーガイド</u>」を参照 してください。

トピック

- ・ にサインアップする AWS
- IAM ユーザーの作成
- 次のステップ

にサインアップする AWS

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

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

サインアップ手順の一環として、通話呼び出しまたはテキストメッセージを受け取り、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。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、<u>ルー トユーザーアクセスが必要なタスク</u>の実行にはルートユーザーのみを使用するようにしてくださ い。

IAM ユーザーの作成

管理者ユーザーを作成するには、以下のいずれかのオプションを選択します。

管理者を管理する方 法を1つ選択します	目的	方法	以下の操作も可能
IAM Identity Center 内 (推奨)	短期の認証情報を使 用して AWSにアクセ スします。 これはセキュリティ のベストプラクティ スと一致しています 。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「 <u>IAM でのセ</u> キュリティのベスト プラクティス」を参 照してください。	AWS IAM Identity Center ユーザーガイ ドの「 <u>開始方法</u> 」の 手順に従います。	AWS Command Line Interface ユーザーガ イドの <u>を使用する</u> AWS CLI ように を設 定 AWS IAM Identity Centerして、プログ ラムによるアクセス を設定します。
IAM 内 (非推奨)	長期認証情報を使用 して AWSにアクセス する。	IAM ユーザーガイ ドの「 <u>最初の IAM 管</u> <u>理者のユーザーおよ</u> <u>びグループの作成</u> 」 の手順に従います。	IAM ユーザーガイ ドの「 <u>IAM ユーザー</u> <u>のアクセスキーの管</u> <u>理</u> 」に従って、プロ グラムによるアクセ スを設定します。

Note

AWSWickrFullAccess マネージドボリシーを割り当てて、Wickr サービスに完全な 管理者権限を付与することもできます。詳細については、「<u>AWS マネージドポリシー:</u> AWSWickrFullAccess」を参照してください。

次のステップ

前提条件となる設定手順が完了しました。Wickr の設定を開始するには、<u>入門</u> を参照してください。

AWS Wickr の使用開始

このガイドでは、ネットワークの作成、ネットワークの設定、ユーザーの作成など、Wickrを始める 方法を紹介します。

トピック

- 前提条件
- ステップ1: ネットワークの構築
- ステップ 2: ネットワークの構成
- ステップ 3: ユーザーを作成して招待する

前提条件

始める前に、以下の前提条件を満たしていることを確認してください:

- Amazon Web Services (AWS) にサインアップします。詳細については、「<u>AWS Wickr 用のセット</u> <u>アップ</u>」を参照してください。
- ・Wickr を管理するために必要なアクセス許可があることを確認してください。詳細については、 「AWS マネージドポリシー: AWSWickrFullAccess」を参照してください。
- Wickr の適切なポートとドメインを許可リストに登録していることを確認してください。詳細については、「Wickr ネットワークのリストを許可するポートとドメイン」を参照してください。

ステップ1: ネットワークの構築

Wickr ネットワークを作成できます。

アカウントの Wickr ネットワークを作成には、以下の手順を実行します。

1. Wickr AWS Management Console のをhttps://console.aws.amazon.com/wickr/で開きます。

Note

Wickr ネットワークを作成したことがない場合は、Wickr サービスの情報ページが表示 されます。1 つ以上の Wickr ネットワークを作成すると、作成したすべての Wickr ネッ トワークのリストビューを含む[ネットワーク]ページが表示されます。

- 2. [ネットワークの作成]を選択します。
- ネットワーク名 テキストボックスにネットワークの名前を入力します。会社名やチーム名な ど、組織のメンバーが認識できる名前を選択します。
- 4. プランを選択します。次のいずれかの Wickr ネットワークプランを選択できます。
 - 標準 管理統制と柔軟性を必要とする中小企業チーム向け。
 - プレミアムまたはプレミアム無料トライアル 最高の機能制限、きめ細かな管理コントロール、データ保持を必要とする企業向け。

管理者は、最大 30 人のユーザーが利用でき、3 か月間有効なプレミアム無料トライアルを選択 できます。For AWS WickrGov のプレミアム無料トライアルオプションでは、最大 50 人のユー ザーを許可し、3 か月間使用できます。プレミアム無料トライアル期間中、管理者はプレミアム プランまたはスタンダードプランにアップグレードまたはダウングレードできます。

利用可能な Wickr プランと料金の詳細については、「Wickr 料金表」 を参照してください。

- (オプション)新しいタグを追加を選択してネットワークにタグを追加します。タグはキーと 値のペアで構成されています。タグは、リソースの検索やフィルタリング、または AWS コスト の追跡に使用できます。詳細については、「ネットワークタグ」を参照してください。
- 6. ネットワークの作成 を選択します。

Wickr AWS Management Console の のネットワークページにリダイレクトされ、新しいネット ワークがページに表示されます。

ステップ 2: ネットワークの構成

Wickr AWS Management Console の にアクセスするには、次の手順を実行します。ここでは、ユー ザーの追加、セキュリティグループの追加、SSO の設定、データ保持の設定、その他のネットワー ク設定を行うことができます。

1. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。

選択したネットワークの Wickr 管理コンソールにリダイレクトされます。

2. 次のユーザー管理オプションを使用できます。これらの設定の実行に関する詳細については、 「AWS Wickr ネットワークの管理」を参照してください。

- セキュリティグループ パスワードの複雑性ポリシー、メッセージ設定、通話機能、セキュリティ機能、外部フェデレーションなどのセキュリティグループとその設定を管理します。詳細については、「AWS Wickr のセキュリティグループ」を参照してください。
- シングルサインオン (SSO) 設定 SSO を設定し、Wickr ネットワークのエンドポイントアドレスを表示します。Wickr は、OpenID Connect (OIDC) を使用する SSO プロバイダーのみをサポートしています。Security Assertion Markup Language (SAML) を使用するプロバイダーはサポートされていません。詳細については、「AWS Wickr のシングルサインオン設定」を参照してください。

ステップ 3: ユーザーを作成して招待する

次の方法を使用して、Wickr ネットワークにユーザーを作成できます。

- シングルサインオン SSO を設定すると、Wickr 会社 ID を共有してユーザーを招待できます。エンドユーザーは、提供された会社 ID と仕事用の E メールアドレスを使用して Wickr に登録します。詳細については、「AWS Wickr のシングルサインオン設定」を参照してください。
- 招待 Wickr AWS Management Console でユーザーを手動で作成し、そのユーザーに招待 E メー ルを送信できます。エンドユーザーは、E メール内のリンクを選択して Wickr に登録できます。

Note

Wickr ネットワークのゲストユーザーを有効にすることもできます。詳細については、<u>AWS</u> Wickr ネットワークのゲストユーザーを参照してください。

ユーザーを作成または招待するには、以下の手順を実行します。

Note

管理者もユーザーと見なされ、SSO または SSO 以外の Wickr ネットワークに自分自身を招 待する必要があります。

Wickr ユーザーを作成し、SSO を使用して招待を送信するには:

Wickr にサインアップする必要がある SSO ユーザーに E メールを書いて送信します。E メールに は、以下の情報を記載してください。

- Wickr の会社 ID。SSO を設定するときに Wickr ネットワークの会社 ID を指定します。詳細については、「AWS Wickr で SSO を設定する」を参照してください。
- サインアップに使用すべき E メールアドレス。
- Wickr クライアントをダウンロードするための URL。ユーザーは <u>https://aws.amazon.com/wickr/</u> download/の AWS Wickr ダウンロードページから Wickr クライアントをダウンロードできます。

Note

AWS GovCloud (米国西部) で Wickr ネットワークを作成した場合は、WickrGov クライア ントをダウンロードしてインストールするようにユーザーに指示します。他のすべての AWS リージョンでは、標準の Wickr クライアントをダウンロードしてインストールする ようにユーザーに指示します。 AWS WickrGov の詳細については、AWS GovCloud (US) 「ユーザーガイド」のAWS WickrGov」を参照してください。

ユーザーが Wickr ネットワークに登録すると、そのユーザーはアクティブのステータスで Wickr チームディレクトリに追加されます。

Wickr ユーザーを手動で作成して招待状を送信するには

- 1. Wickr AWS Management Console のをhttps://console.aws.amazon.com/wickr/で開きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。

Wickr ネットワークにリダイレクトされます。Wickr ネットワークでは、ユーザーの追加、セ キュリティグループの追加、SSO の設定、データ保持の設定、追加設定の調整を行うことがで きます。

- 3. ナビゲーションペインで、ユーザー管理を選択します。
- 4. ユーザー管理ページのチームディレクトリタブで、ユーザーを招待を選択します。

招待ユーザーの横にあるドロップダウン矢印を選択して、ユーザーを一括招待することもできま す。ユーザーを一括招待ページで、テンプレートのダウンロードを選択して、ユーザーのリスト で編集およびアップロードできる CSV テンプレートをダウンロードします。

5. ユーザーの名、姓、国コード、電話番号、Eメールアドレスを入力します。必須のフィールドは Eメールアドレスだけです。ユーザーに適したセキュリティグループを必ず選択してください。 6. [招待]を選択します。

Wickr は、ユーザーに指定したアドレスに招待 E メールを送信します。この E メールに は、Wickr クライアントアプリケーションのダウンロードリンクと Wickr に登録するためのリ ンクが記載されています。このエンドユーザーエクスペリエンスの詳細については、「AWS Wickr ユーザーガイド」の「<u>Wickr アプリをダウンロードして招待を受ける</u>」を参照してくださ い。

ユーザーが E メール内のリンクを使用して Wickr に登録すると、Wickr チームディレクトリの ステータスが [保留中] から [アクティブ] に変わります。

次のステップ

スタートアップの手順は完了しました。Wickr を管理するには、以下を参照してください。

- AWS Wickr ネットワークの管理
- AWS Wickr でユーザーを管理する

AWS Wickr ネットワークの管理

AWS Management Console for Wickr では、Wickr ネットワーク名、セキュリティグループ、SSO 設 定、データ保持設定を管理できます。

トピック

- AWS Wickr のネットワークの詳細
- AWS Wickr のセキュリティグループ
- AWS Wickr のシングルサインオン設定
- AWS Wickr のネットワークタグ
- AWS Wickr の領収書の読み取り
- AWS Wickr のネットワークプランを管理する
- AWS Wickr のデータ保持
- ATAK とは
- Wickr ネットワークのリストを許可するポートとドメイン
- GovCloud クロス境界分類とフェデレーション
- ・ AWS Wickr のファイルプレビュー

AWS Wickr のネットワークの詳細

Wickr ネットワークの名前を編集し、Wickr AWS Management Console の のネットワークの詳細セ クションでネットワーク ID を表示できます。

トピック

- <u>AWS Wickr でネットワークの詳細を表示する</u>
- AWS Wickr でネットワーク名を編集する
- AWS Wickr でネットワークを削除する

AWS Wickr でネットワークの詳細を表示する

ネットワーク名やネットワーク ID など、Wickr ネットワークの詳細を表示できます。

Wickr ネットワークプロファイルとネットワーク ID を表示するには、以下の手順を実行します。

- 1. Wickr AWS Management Consoleのをhttps://console.aws.amazon.com/wickr/で開きます。
- 2. ネットワークページで、表示するネットワークを見つけます。
- 表示するネットワークの右側で、縦の省略記号アイコン (3 つのドット)を選択し、詳細の表示を選択します。

Network ホームページには、Wickr ネットワーク名とネットワーク ID が Network details セク ションに表示されます。ネットワーク ID を使用してフェデレーションを設定できます。

AWS Wickr でネットワーク名を編集する

Wickr ネットワークの名前を編集できます。

Wickr ネットワーク名を編集するには、以下の手順を実行します。

- 1. Wickr AWS Management Console のをhttps://console.aws.amazon.com/wickr/で開きます。
- ネットワークページで、ネットワーク名を選択して、そのネットワークの Wickr 管理コンソー ルに移動します。
- 3. ネットワークホームページのネットワークの詳細セクションで、編集を選択します。
- 4. [ネットワーク名] テキストボックスに新しいネットワーク名を入力します。
- 5. 保存を選択して、新しいネットワーク名を保存します。

AWS Wickr でネットワークを削除する

AWS Wickr ネットワークを削除できます。

プレミアム無料トライアルネットワークを削除した場合、別の無料トライアルネットワーク を作成することはできません。

ネットワークホームページで Wickr ネットワークを削除するには、次の手順を実行します。

- 1. Wickr AWS Management Console のをhttps://console.aws.amazon.com/wickr/で開きます。
- 2. ネットワークページで、削除するネットワークを見つけます。
- 1. 削除するネットワークの右側で、縦の省略記号アイコン (3 つのドット)を選択し、ネットワークの削除を選択します。

¹ Note

4. ポップアップウィンドウで「確認」と入力し、「削除」を選択します。

ネットワークが削除されるまでに数分かかる場合があります。

ネットワーク内で Wickr ネットワークを削除するには、次の手順を実行します。

- 1. Wickr AWS Management Console のをhttps://console.aws.amazon.com/wickr/で開きます。
- 2. ネットワークページで、削除するネットワークを選択します。
- 3. ネットワークホームページの右上隅近くで、ネットワークの削除を選択します。
- 4. ポップアップウィンドウで「確認」と入力し、「削除」を選択します。

ネットワークが削除されるまでに数分かかる場合があります。

Note

データ保持設定 (有効になっている場合) によって保持されているデータは、ネットワー クを削除しても削除されません。詳細については、<u>「AWS Wickr のデータ保持</u>」を参照 してください。

AWS Wickr のセキュリティグループ

Wickr AWS Management Console の のセキュリティグループセクションでは、パスワードの複雑さ に関するポリシー、メッセージング設定、通話機能、セキュリティ機能、ネットワークフェデレー ションなど、セキュリティグループとその設定を管理できます。

トピック

- AWS Wickr でセキュリティグループを表示する
- AWS Wickr でセキュリティグループを作成する
- AWS Wickr でセキュリティグループを編集する
- AWS Wickr でセキュリティグループを削除する

AWS Wickr でセキュリティグループを表示する

Wickr セキュリティグループの詳細を表示できます。

セキュリティグループを表示するには、以下の手順を実行します。

- 1. Wickr AWS Management Console のをhttps://console.aws.amazon.com/wickr/で開きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、[Security Groups] (セキュリティグループ) を選択します。

セキュリティグループページには、現在の Wickr セキュリティグループが表示され、新しいグ ループを作成するオプションが表示されます。

セキュリティグループページで、表示するセキュリティグループを選択します。このページに は、そのセキュリティグループの現在の詳細が表示されます。

AWS Wickr でセキュリティグループを作成する

新しい Wickr セキュリティグループを作成できます。

以下の手順でセキュリティグループを作成します。

- 1. Wickr AWS Management Console のをhttps://console.aws.amazon.com/wickr/で開きます。
- ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、[Security Groups] (セキュリティグループ) を選択します。
- セキュリティグループページで、セキュリティグループの作成を選択して新しいセキュリティグ ループを作成します。

Note

デフォルト名の新しいセキュリティグループがセキュリティグループリストに自動的に 追加されます。

- 5. セキュリティグループの作成ページで、セキュリティグループの名前を入力します。
- 6. [セキュリティグループの作成]を選択してください。

新しいセキュリティグループの編集の詳細については、<u>AWS Wickr でセキュリティグループを</u> 編集するを参照してください。

AWS Wickr でセキュリティグループを編集する

Wickr セキュリティグループの詳細を編集できます。

セキュリティグループを編集するには、以下の手順を実行します。

- 1. Wickr AWS Management Console のをhttps://console.aws.amazon.com/wickr/で開きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、[Security Groups] (セキュリティグループ) を選択します。
- 4. 編集するセキュリティグループの名前を選択します。

セキュリティグループの詳細ページには、セキュリティグループの設定がさまざまなタブに表示 されます。

- 5. 次のタブと対応する設定を使用できます。
 - セキュリティグループの詳細 セキュリティグループの詳細セクションで編集を選択して名前を編集します。
 - メッセージング: グループメンバーのメッセージ機能を管理します。
 - Burn-on-read Wickr クライアントのburn-on-readタイマーにユーザーが設定できる最大値 を制御します。詳細については、「Wickr クライアントでメッセージの有効期限とバーンタ イマーを設定する」を参照してください。
 - 有効期限タイマー Wickr クライアントでユーザーがメッセージの有効期限タイマーに設 定できる最大値を制御します。詳細については、「Wickr クライアントでメッセージの有効 期限とバーンタイマーを設定する」を参照してください。
 - クイックレスポンス ユーザーがメッセージに応答するためのクイックレスポンスのリストを設定します。
 - セキュアシュレッダーの強度 ユーザーに対してセキュアシュレッダーコントロールを実行する頻度を設定します。詳細については、「メッセージング」を参照してください。
 - 通話: グループメンバーの通話機能を管理します。
 - 音声通話を有効にする ユーザーは音声通話を開始できます。
 - ビデオ通話と画面共有を有効にする ユーザーは通話中にビデオ通話を開始したり画面を 共有したりできます。
 - TCP 呼び出し TCP 呼び出しの有効化 (または強制) は通常、組織の IT 部門またはセキュリティ部門によって標準の VoIP UDP ポートが許可されていない場合に使用されます。TCP 呼び出しが無効になっており、UDP ポートを使用できない場合、Wickr クライアントは最初に UDP を試し、TCP にフォールバックします。
 - メディアとリンク グループのメンバーのメディアとリンクに関連する設定を管理します。

ファイルのダウンロードサイズ — 最高品質の転送を選択して、ユーザーが元の暗号化さ れた形式でファイルと添付ファイルを転送できるようにします。低帯域幅転送を選択する と、Wickr のユーザーによって送信されたファイル添付ファイルは Wickr ファイル転送サービ スによって圧縮されます。

Location — グループのメンバーのロケーション共有設定を管理します。

ロケーション共有 — ユーザーは GPS 対応デバイスを使用してロケーションを共有できま す。この機能は、デバイスのオペレーティングシステムのデフォルトに基づいてビジュアル マップを表示します。ユーザーはマップビューを無効にし、代わりに GPS 座標を含むリンク を共有できます。

- セキュリティ: グループに追加のセキュリティ機能を設定します。
 - アカウント乗っ取り保護を有効にする ユーザーがアカウントに新しいデバイスを追加するときに、2 要素認証を適用します。新しいデバイスを検証するには、古いデバイスからWickr コードを生成するか、E メール検証を実行できます。これは、AWS Wickr アカウントへの不正アクセスを防ぐためのセキュリティの追加レイヤーです。
 - 常に再認証を有効にする アプリケーションに再入力するときに、ユーザーに常に再認証 を強制します。
 - マスターリカバリキー アカウントの作成時にマスターリカバリキーを作成します。他の デバイスが使用できない場合、ユーザーは自分のアカウントへの新しいデバイスの追加を承 認できます。
- 通知と可視性 グループのメンバーへの通知でメッセージプレビューなどの通知と可視性の 設定を行います。
- ・ Wickr オープンアクセス グループのメンバーの Wickr オープンアクセス設定を構成します。
 - Wickr オープンアクセスを有効にする Wickr オープンアクセスを有効にすると、トラフィックを偽装して、制限された監視対象ネットワーク上のデータを保護します。地理的位置に基づいて、Wickr オープンアクセスは、トラフィックの難読化に最適なパスとプロトコルを提供するさまざまなグローバルプロキシサーバーに接続します。
 - Force Wickr open access すべてのデバイスで Wickr open access を自動的に有効化して 適用します。
- フェデレーション ユーザーが他の Wickr ネットワークと通信できるかどうかを制御します。
 - ローカルフェデレーション 同じリージョン内の他のネットワークの AWS ユーザーと フェデレーションする機能。たとえば、ローカルフェデレーションが有効になっているカ ナダ (中部) リージョンに AWS 2 つのネットワークがある場合、それらは相互に通信できま す。

- グローバルフェデレーション Wickr Enterprise ユーザーまたは他のリージョンに属する 別のネットワークの AWS ユーザーとフェデレーションする機能。たとえば、カナダ (中部) リージョンの AWS Wickr ネットワーク上のユーザーと、欧州 (ロンドン) リージョンのネッ トワーク内の AWS ユーザーは、両方のネットワークでグローバルフェデレーションがオ ンになっているときに相互に通信できます。
- 制限付きフェデレーション ユーザーがフェデレーションできる特定の AWS Wickr また は Wickr Enterprise ネットワークのリストを許可します。設定すると、ユーザーは許可リス トに登録されたネットワーク内の外部ユーザーとのみ通信できます。どちらのネットワーク でも、制限付きフェデレーションを使用するには、相互にリストを許可する必要がありま す。

ゲストフェデレーションの詳細については、<u>「AWS Wickr ネットワークでゲストユーザー</u> を有効または無効にする」を参照してください。

- ATAK プラグイン設定 ATAK の有効化の詳細については、「<u>ATAK とは</u>」を参照してくだ さい。
- 6. 保存を選択して、セキュリティグループの詳細に加えた編集を保存します。

AWS Wickr でセキュリティグループを削除する

Wickr セキュリティグループを削除できます。

セキュリティグループを削除するには、以下の手順に従ってください。

- 1. Wickr AWS Management Console のをhttps://console.aws.amazon.com/wickr/で開きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、[Security Groups] (セキュリティグループ) を選択します。
- 4. セキュリティグループページで、削除するセキュリティグループを見つけます。
- 5. 削除するセキュリティグループの右側で、縦の省略記号アイコン (3 つのドット)を選択し、削除を選択します。
- 6. ポップアップウィンドウで「確認」と入力し、「削除」を選択します。

ユーザーが割り当てられているセキュリティグループを削除すると、そのユーザーはデフォルト のセキュリティグループに自動的に追加されます。ユーザーに割り当てられたセキュリティグ ループを変更するには、「<u>AWS Wickr ネットワークでユーザーを編集する</u>」を参照してくださ い。

AWS Wickr のシングルサインオン設定

Wickr AWS Management Console の では、シングルサインオンシステムを使用して認証するよう に Wickr を設定できます。SSO は、適切な多要素認証 (MFA) システムと組み合わせると、セキュリ ティを強化します。Wickr は、OpenID Connect (OIDC) を使用する SSO プロバイダーのみをサポー トしています。Security Assertion Markup Language (SAML) を使用するプロバイダーはサポートさ れていません。

トピック

- AWS Wickr で SSO の詳細を表示する
- AWS Wickr で SSO を設定する
- トークン更新の猶予期間

AWS Wickr で SSO の詳細を表示する

Wickr ネットワークとネットワークエンドポイントのシングルサインオン設定の詳細を表示できます。

Wickr ネットワークの現在のシングルサインオン設定を表示するには、次の手順を実行します。

- 1. Wickr AWS Management Consoleのをhttps://console.aws.amazon.com/wickr/で開きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、ユーザー管理を選択します。

ユーザー管理ページで、シングルサインオンセクションに Wickr ネットワークエンドポイント と現在の SSO 設定が表示されます。

AWS Wickr で SSO を設定する

Wickr ネットワークへの安全なアクセスを確保するために、現在のシングルサインオン設定をセット アップできます。このプロセスに役立つ詳細なガイドが用意されています。

SSO の設定の詳細については、以下のガイドを参照してください。

▲ Important

SSO を設定するときに Wickr ネットワークの会社 ID を指定します。Wickr ネットワークの 会社 ID を必ず書き留めてください。招待 E メールを送信するときは、エンドユーザーに提 供する必要があります。エンドユーザーは、Wickr ネットワークに登録する際に会社 ID を指 定する必要があります。

- Microsoft Entra (Azure AD) を使用した AWS Wickr シングルサインオン (SSO) のセットアップ
- ・ Okta を使用した AWS Wickr シングルサインオン (SSO) のセットアップ
- Amazon Cognito を使用した AWS Wickr シングルサインオン (SSO) のセットアップ

Microsoft Entra (Azure AD) シングルサインオンで AWS Wickr を設定する

AWS Wickr は、Microsoft Entra (Azure AD) を ID プロバイダーとして使用するように設定できま す。そのためには、Microsoft Entra と AWS Wickr 管理コンソールの両方で次の手順を実行します。

A Warning

ネットワークで SSO を有効にすると、Wickr からアクティブなユーザーに署名し、SSO プ ロバイダーを使用して再認証するように強制します。

ステップ 1: Microsoft Entra でアプリケーションとして AWS Wickr を登録する

Microsoft Entra でアプリケーションとして AWS Wickr を登録するには、次の手順を実行します。

Note

詳細なスクリーンショットとトラブルシューティングについては、Microsoft Entra のドキュ メントを参照してください。詳細については、<u>「Microsoft ID プラットフォームでアプリ</u> <u>ケーションを登録する</u>」を参照してください。

- 1. ナビゲーションペインで、アプリケーションを選択し、アプリケーション登録を選択します。
- 2. アプリ登録ページで、アプリケーションの登録を選択し、アプリケーション名を入力します。

- この組織ディレクトリのアカウントのみを選択します (デフォルトディレクトリのみ シングル テナント)。
- リダイレクト URI で、ウェブを選択し、次のウェブアドレスを入力します: https:// messaging-pro-prod.wickr.com/deeplink/oidc.php。

Note

リダイレクト URI は、AWS Wickr 管理者コンソールの SSO 設定からコピーすることも できます。

- 5. [登録]を選択します。
- 6. 登録後、生成されたアプリケーション (クライアント) ID をコピー/保存します。



- 7. エンドポイントタブを選択して、次の点を書き留めます。
 - Oauth 2.0 認可エンドポイント (v2): 例: https:// login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/ oauth2/v2.0/authorize
 - 2. この値を編集して「oauth2/」と「authorize」を削除します。たとえば、固定 URL は次の ようになります。https://login.microsoftonline.com/1ce43025-e4b1-462da39f-337f20f1f4e1/v2.0/
 - 3. これは SSO 発行者として参照されます。

ステップ 2: 認証を設定する

Microsoft Entra で認証を設定するには、次の手順を実行します。

- 1. ナビゲーションペインで、認証を選択します。
- 認証ページで、ウェブリダイレクト URI が以前に入力したものと同じであることを確認します (アプリケーションとして AWS Wickr を登録する)。

Wickr-test-asb Authentication					
₽ Search «	🖗 Got feedback?				
Overview	Platform configurations				
4 Quickstart	Depending on the platform or device this application is targeting, add	litional configuration may be required such as			
💉 Integration assistant	realiect ons, specific admenication settings, or news specific to the pa	alorn.			
X Diagnose and solve problems	+ Add a platform				
Manage		Quickstart Decce?			
😑 Branding & properties	Redirect URIs				
Authentication	The URIs we will accept as destinations when returning authentication	on responses (tokens) after successfully			
Certificates & secrets	authenticating or signing out users. The redirect URI you send in the match one listed here. Also referred to as reply URLs. Learn more ab	request to the login server should out Redirect URIs and their restrictions			
Token configuration	ď				
 API permissions 	https://messaging-pro-beta.secmv.net/deeplink/oidc.php	ii ii			

- Select 暗黙的なフローに使用されるアクセストークンと、暗黙的なフローとハイブリッドフローに使用される ID トークンを選択します。
- 4. [保存]を選択します。

Chaptiene .	
	Implicit grant and hybrid flows
 Quickstart 	Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and
🚀 Integration assistant	doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn
X Diagnose and solve problems	more about tokens.
Manage	Select the tokens you would like to be issued by the authorization endpoint:
Branding & properties	Access tokens (used for implicit flows)
Authentication	ID tokens (used for implicit and hybrid flows)
📍 Certificates & secrets	Supported account types
Token configuration	Who can use this application or access this API?
API permissions	 Accounts in this organizational directory only (Default Directory only - Single tenant)
🛆 Expose an API	 Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
15 App roles	Save
🚨 Owners .	

ステップ 3: 証明書とシークレットを設定する

Microsoft Entra で証明書とシークレットを設定するには、次の手順を実行します。

- 1. ナビゲーションペインで、証明書とシークレットを選択します。
- 2. 証明書とシークレットページで、クライアントシークレットタブを選択します。
- 3. クライアントシークレットタブで、新しいクライアントシークレットを選択します。
- 4. 説明を入力し、シークレットの有効期限を選択します。

5. [Add] (追加)を選択します。

Add a client secret		×
Description	NewCl1entsecret	
Expires	730 days (24 months)	~
Add Cancel		

6. 証明書を作成したら、クライアントシークレット値をコピーします。

Wickr Client Secret	7/23/2026	vcm8Q~3XalXfGO5nl	16W D 52400f1c-c02e	:d5a803e78 🗈 📋
			2100	

Note

クライアントアプリケーションコードには、クライアントシークレット値 (シークレット ID ではない) が必要です。このページを離れると、シークレット値を表示またはコ ピーできない場合があります。今すぐコピーしない場合は、戻って新しいクライアント シークレットを作成する必要があります。

ステップ 4: トークン設定をセットアップする

Microsoft Entra でトークン設定をセットアップするには、次の手順を実行します。

- 1. ナビゲーションペインで、トークン設定を選択します。
- 2. トークン設定ページで、オプションのクレームの追加を選択します。
- 3. オプションのクレームで、ID としてトークンタイプを選択します。
- 4. ID を選択したら、クレームで E メールとアップグレードを選択します。
- 5. [Add] (追加)を選択します。

Optional claims					
Optional claims are used to configure additional information which is returned in one or more tokens. Learn more 🖉					
+ Add optional claim + Add	groups claim				
				12	
Claim 1	Description	Token type ↑↓	Optional settings		
Claim ↑↓ email	Description The addressable email for this user, if the user has one	Token type ↑↓ ID	Optional settings		
Claim †u email upn	Description The addressable email for this user, if the user has one An identifier for the user that can be used with the username_hint parameter; not a durable identifier for the user and sho	Token type ↑↓ ID ID	Optional settings - Default		

ステップ 5: API アクセス許可を設定する

Microsoft Entra で API アクセス許可を設定するには、次の手順を実行します。

- 1. ナビゲーションペインで、[API permissions] (API アクセス許可)を選択します。
- 2. API アクセス許可ページで、アクセス許可の追加を選択します。

	API	permissions 🖈 …	×
P Search) «	🕐 Refresh 🔰 🖗 Got feedback?	
 Diagnose and solve problems Manage 	•	The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more	e î
 Branding & properties Authentication 	ł	Configured permissions Applications are authorized to call APIs when they are granted permissions by users/admins as part of the con-	sent
📍 Certificates & secrets		process. The list of configured permissions should include all the permissions the application needs. Learn mor permissions and consent	re about
Token configuration			
 API permissions 		+ Add a permission V Grant admin consent for Default Directory	
🛆 Expose an API		API / Permissions na Add a permission Description Adm	nin cons
App roles		V Microsoft Graph (1)	
🚨 Owners		User.Read Delegated Sign in and read user profile No	
a. Roles and administrators		¢	+

- 3. Microsoft Graph を選択し、委任されたアクセス許可を選択します。
- 4. Eメール、オフラインアクセス、openid、プロファイルのチェックボックスをオンにします。
- 5. [Add permissions (許可の追加)] を選択します。

ステップ 6: API を公開する

Microsoft Entra の 4 つのスコープのそれぞれに API を公開するには、次の手順を実行します。

- 1. ナビゲーションペインで、API を公開を選択します。
- 2. APIを公開ページで、スコープの追加を選択します。

60	Wickr-test-asb Expose an API 🛛 🖈 🐇				×	
٩	Search	~	R Got feedback?			
Ma	nage	*	Define custom scopes to restrict access	to data and functionality protected b	w the API. An application th	hat requires
	Branding & properties		access to parts of this API can request t	that a user or admin consent to one o	r more of these.	an equilation of the second
Э	Authentication		Adding a scope here creates only deleg 'App roles' and define app roles assign:	gated permissions. If you are looking t able to application type, Go to App ro	to create application-only s	copes, use
Ŷ	Certificates & secrets					
11	Token configuration	- 1	+ Add a scope			
٠	API permissions		Scopes Add a scope	Who can consent	Admin consent disp	User consent
4	Expose an API		No scopes have been defined			
82	App roles		€			•
24	Owners		A 11 1 1 1 1 1 1 1			

アプリケーション ID URI は自動的に入力され、URI に続く ID はアプリケーション ID (アプリ ケーションとして AWS Wickr を登録する で作成) と一致する必要があります。

Add a scope	×
You'll need to set an Application ID URI before you can add a permission. We've chosen o but you can change it. Application ID URI * ①	one,
api://00a720cd-cf03- 92a679b85	
Save and continue Cancel	

- 3. [Save and continue] を選択します。
- 4. Admins and users タグを選択し、スコープ名を offline_access として入力します。
- 5. 状態を選択し、有効化を選択します。
- 6. スコープの追加を選択します。
- このセクションのステップ1~6を繰り返して、Eメール、openid、プロファイルのスコープを 追加します。

Application ID URI : api://00a720cd-cf03-4203-ad69-fd592a679b85							
Scopes defined by this API							
Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.							
Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to application type. Go to App roles.							
+ Add a scope							
Scopes		Who can consent	Admin consent display	User consent display na	State		
api://00a720cd	679b85/offlin	Admins and users	offline access		for a balance		
		-	onnie_access		Enabled		
api://00a720cd-	679b85/email	Admins and users	email		Enabled		
api://00a720cd-	679b85/email	Admins and users Admins and users	email openid		Enabled Enabled Enabled		
api://00a720cd- api://00a720cd- api://00a720cd-	679b85/email 🕅 679b85/openid 🕅 679b85/profile 🕅	Admins and users Admins and users Admins and users	email openid profile		Enabled Enabled Enabled		

- 8. 「承認されたクライアントアプリケーション」で、「クライアントアプリケーションの追加」を 選択します。
- 9. 前のステップで作成した4つのスコープをすべて選択します。
- 10. アプリケーション (クライアント) ID を入力または検証します。
- 11. [アプリケーションの追加]を選択します。

ステップ 7: AWS Wickr SSO 設定

AWS Wickr コンソールで次の設定手順を実行します。

- 1. Wickr AWS Management Console の を<u>https://console.aws.amazon.com/wickr/</u>://www.」で開き ます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、ユーザー管理を選択し、SSOの設定を選択します。
- ネットワークエンドポイントで、リダイレクト URI が次のウェブアドレスと一致することを確認します (ステップ 4 でアプリケーションとして AWS Wickr を登録するで追加)。

https://messaging-pro-prod.wickr.com/deeplink/oidc.php.

- 5. 次の詳細情報を入力します。
 - 発行者 これは以前に変更されたエンドポイントです(例: https:// login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/ v2.0/)。

- クライアント ID これは概要ペインのアプリケーション (クライアント) ID です。
- クライアントシークレット (オプション) これは、証明書とシークレットペインのクライ アントシークレットです。
- スコープ API ペインに公開されているスコープ名です。E メール、プロファイル、オフラ インアクセス、openid を入力します。
- カスタムユーザー名スコープ (オプション) upn と入力します。
- 会社 ID 英数字とアンダースコア文字を含む一意のテキスト値にすることができます。このフレーズは、新しいデバイスに登録するときにユーザーが入力するものです。

その他のフィールドはオプションです。

- 6. [次へ]を選択します。
- 7. レビューと保存ページで詳細を確認し、変更の保存を選択します。

SSO 設定が完了しました。確認するために、Microsoft Entra のアプリケーションにユーザーを追加 し、SSO と会社 ID を使用してユーザーでログインできるようになりました。

ユーザーを招待およびオンボードする方法の詳細については、<u>「ユーザーの作成と招待</u>」を参照して ください。

トラブルシューティング

以下は、発生する可能性のある一般的な問題と、それらを解決するための提案です。

- SSO 接続テストが失敗するか、応答しません。
 - SSO 発行者が想定どおりに設定されていることを確認します。
 - SSO Configured の必須フィールドが想定どおりに設定されていることを確認します。
- 接続テストは成功しましたが、ユーザーはログインできません。
 - Microsoft Entra に登録した Wickr アプリケーションにユーザーが追加されていることを確認します。
 - ユーザーがプレフィックスを含む正しい会社 ID を使用していることを確認します。例: UE1-DemoNetworkW_drqtva。
 - AWS Wickr SSO 設定でクライアントシークレットが正しく設定されていない可能性があります。Microsoft Entra で別のクライアントシークレットを作成して再設定し、Wickr SSO 設定で新しいクライアントシークレットを設定します。

トークン更新の猶予期間

ID プロバイダーが一時的または長期的に停止し、クライアントセッションの更新トークンが失敗し たためにユーザーが予期せずログアウトすることがあります。この問題を防ぐには、停止中にクライ アント更新トークンに障害が発生しても、ユーザーがサインインしたままになる猶予期間を設定でき ます。

猶予期間に使用できるオプションは次のとおりです。

- 猶予期間なし(デフォルト): 更新トークンが失敗すると、ユーザーはすぐにサインアウトされます。
- 30 分の猶予期間: 更新トークンが失敗した後も、ユーザーは最大 30 分間サインインしたままになります。
- 60 分の猶予期間: 更新トークンが失敗した後も、ユーザーは最大 60 分間サインインしたままになります。

AWS Wickr のネットワークタグ

Wickr ネットワークにタグを適用できます。その後、これらのタグを使用して Wickr ネットワー クを検索およびフィルタリングしたり、 AWS コストを追跡したりできます。 AWS Management Console for Wickr の Network ホームページでネットワークタグを設定できます。

タグはリソースに適用される <u>[キーと値のペア]</u> で、そのリソースに関するメタデータを保持しま す。各タグは、キーと値からなるラベルです。タグの詳細については、「<u>タグとは</u>」および「<u>タグ付</u> けのユースケース」も参照してください。

トピック

- AWS Wickr でネットワークタグを管理する
- AWS Wickr でネットワークタグを追加する
- AWS Wickr でネットワークタグを編集する
- AWS Wickr でネットワークタグを削除する

AWS Wickr でネットワークタグを管理する

Wickr ネットワークのネットワークタグを管理できます。

Wickr ネットワークのネットワークタグを管理するには、以下の手順を実行します。

- 1. Wickr AWS Management Console のをhttps://console.aws.amazon.com/wickr/で開きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ネットワークのホームページの「タグ」セクションで、「タグの管理」を選択します。
- 4. タグの管理ページで、次のいずれかのオプションを実行できます。
 - 新しいタグの追加:新しいタグをキーと値のペアの形式で入力します。[新しいタグの追加]を 選択して、複数のキーと値のペアを追加します。タグは、大文字と小文字が区別します。詳細 については、「AWS Wickr でネットワークタグを追加する」を参照してください。
 - 既存のタグの編集: 既存のタグのキーまたは値のテキストを選択し、テキストボックスに変更 内容を入力します。詳細については、「<u>AWS Wickr でネットワークタグを編集する</u>」を参照 してください。
 - 既存のタグの削除: 削除するタグの横に表示されている 削除 ボタンを選択します。詳細については、「AWS Wickr でネットワークタグを削除する」を参照してください。

AWS Wickr でネットワークタグを追加する

Wickr ネットワークにネットワークタグを追加できます。

Wickr ネットワークにタグを追加するには、以下の手順を実行します。タグの管理の詳細について は、「AWS Wickr でネットワークタグを管理する」を参照してください。

- 1. ネットワークのホームページの「タグ」セクションで、「新しいタグの追加」を選択します。
- 2. [タグの管理]ページで、[タグの追加]を選択します。
- 3. 表示される空の [キー] フィールドと [値] フィールドに、新しいタグキーと値を入力します。
- 4. [変更の保存]を選択して設定を保存します。

AWS Wickr でネットワークタグを編集する

Wickr ネットワークにネットワークタグを編集できます。

Wickr ネットワークに関連付けられたタグをの編集するには、以下の手順を実行します。タグの管理 の詳細については、「<u>AWS Wickr でネットワークタグを管理する</u>」を参照してください。

1. [タグの管理] ページで、タグの値を編集します。

Note

タグのキーは編集できません。代わりに、キーと値のペアを削除し、新しいキーを使用 して新しいタグを追加してください。

2. [変更の保存]を選択してタグを保存します。

AWS Wickr でネットワークタグを削除する

Wickr ネットワークへのネットワークタグを削除できます。

Wickr ネットワークにタグを削除するには、以下の手順を実行します。タグの管理の詳細について は、「AWS Wickr でネットワークタグを管理する」を参照してください。

1. [タグの管理] ページで、削除する各タグの横にある [削除] を選択します。

2. [変更の保存]を選択してタグを保存します。

AWS Wickr の領収書の読み取り

AWS Wickr の読み取り受信は、メッセージがいつ読み取られたかを示すために送信者に送信される 通知です。これらの受信は、one-on-one の会話で利用できます。送信されたメッセージには 1 つの チェックマークが表示され、読み取りメッセージにはチェックマークが付いた実線の円が表示されま す。外部会話中にメッセージの読み取り受信を表示するには、両方のネットワークで読み取り受信が 有効になっている必要があります。

管理者は、管理者パネルで読み取り受信を有効または無効にできます。この設定はネットワーク全体 に適用されます。

読み取り受信を有効または無効にするには、次の手順を実行します。

- 1. Wickr AWS Management Console のをhttps://console.aws.amazon.com/wickr/で開きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、ネットワークポリシーを選択します。
- 4. ネットワークポリシーページのメッセージングセクションで、編集を選択します。
- 5. チェックボックスをオンにして、読み取り受信を有効または無効にします。

6. [Save changes] (変更の保存) をクリックします。

AWS Wickr のネットワークプランを管理する

Wickr AWS Management Console の では、ビジネスニーズに基づいてネットワークプランを管理で きます。

ネットワークプランを管理するには、次の手順を実行します。

- 1. Wickr AWS Management Console のをhttps://console.aws.amazon.com/wickr/で開きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ネットワークホームページのネットワークの詳細セクションで、編集を選択します。
- ネットワークの詳細の編集ページで、目的のネットワークプランを選択します。次のいずれかを 選択して、現在のネットワークプランを変更できます。
 - 標準 管理統制と柔軟性を必要とする中小企業チーム向け。
 - プレミアムまたはプレミアム無料トライアル 最高の機能制限、きめ細かな管理コントロール、データ保持を必要とする企業向け。

管理者は、最大 30 人のユーザーが利用でき、3 か月間有効なプレミアム無料トライアルを選 択できます。WickrGov AWS の場合、プレミアム無料トライアルオプションでは最大 50 人の ユーザーが許可され、3 か月間使用できます。このオファーは、新規および標準プランでご利 用いただけます。プレミアム無料トライアル期間中、管理者はプレミアムプランまたはスタン ダードプランにアップグレードまたはダウングレードできます。

Note

ネットワークの使用状況と請求を停止するには、ネットワークから中断されたユー ザーを含め、すべてのユーザーを削除します。

プレミアム無料トライアルの制限

プレミアム無料トライアルには、次の制限が適用されます。

以前にプレミアム無料トライアルに登録されたことがあるプランは、別のトライアルの対象にはなりません。
- プレミアム無料トライアルに登録できるのは、AWS アカウントごとに1つのネットワークのみです。
- ゲストユーザー機能は、プレミアム無料トライアル中は利用できません。
- 標準ネットワークに 30 人を超えるユーザー (WickrGov では AWS 50 人を超えるユーザー) がいる 場合、プレミアム無料トライアルにアップグレードすることはできません。

AWS Wickr のデータ保持

AWS Wickr データ保持では、ネットワーク内のすべての会話を保持できます。これには、直接 的なメッセージの会話や、ネットワーク内 (内部) のメンバーと、ネットワークが連携している 他のチーム (外部) のメンバーとの間でのグループやルームでの会話が含まれます。データ保持 は、AWS Wickr Premium プランのユーザーと、データ保持を選択した企業のお客様のみが利用でき ます。Premium プランの詳細については、「Wickr 料金表」を参照してください。

ネットワーク管理者がネットワークのデータ保持を設定して有効にすると、ネットワーク内で共有す るすべてのメッセージとファイルは、組織のコンプライアンスポリシーに従って保持されます。これ らの .txt ファイル出力には、外部の場所(ローカルストレージ、Amazon S3 バケット、またはユー ザーが選択したその他のストレージ)からネットワーク管理者がアクセスでき、そこから分析、消 去、または転送できます。

Note

Wickr がメッセージやファイルにアクセスすることはありません。したがって、データ保持 システムを設定するのはユーザーの責任です。

トピック

- AWS Wickr でデータ保持の詳細を表示する
- AWS Wickr のデータ保持を設定する
- Wickr ネットワークのデータ保持ログを取得する
- Wickr ネットワークのデータ保持メトリクスとイベント

AWS Wickr でデータ保持の詳細を表示する

Wickr ネットワークのデータ保持の詳細を表示するには、以下の手順を実行します。Wickr ネット ワークのデータ保持を有効または無効にすることもできます。

- 1. Wickr AWS Management Console のをhttps://console.aws.amazon.com/wickr/で開きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、ネットワークポリシーを選択します。
- ネットワークポリシーページには、データ保持を設定する手順と、データ保持機能を有効または 無効にするオプションが表示されます。データ保持の設定については、「<u>AWS Wickr のデータ</u> 保持を設定する」を参照してください。

Note

データ保持機能を有効にすると、データ保持がオンになっています というメッセージがネッ トワーク内のすべてのユーザーに表示され、保持が有効なネットワークであることが通知さ れます。

AWS Wickr のデータ保持を設定する

AWS Wickr ネットワークのデータ保持を設定するには、データ保持ボット Docker イメージを、 ローカルコンピュータや Amazon Elastic Compute Cloud (Amazon EC2) 内のインスタンスなどのホ スト上のコンテナにデプロイする必要があります。ボットをデプロイしたら、データをローカルまた は Amazon Simple Storage Service (Amazon S3) バケットに格納するように設定できます。(Secrets Manager)、Amazon CloudWatch AWS Secrets Manager (CloudWatch)、Amazon Simple Notification Service (Amazon SNS)、() AWS Key Management Service などの他の AWS サービスを使用する ようにデータ保持ボットを設定することもできますAWS KMS。以下のトピックでは、Wickr ネット ワークのデータ保持ボットを設定して実行する方法について説明します。

トピック

- AWS Wickr のデータ保持を設定するための前提条件
- AWS Wickr のデータ保持ボットのパスワード
- AWS Wickr ネットワークのストレージオプション
- AWS Wickr でデータ保持ボットを設定する環境変数
- AWS Wickr の Secrets Manager 値
- ・ AWS サービスでデータ保持を使用するための IAM ポリシー
- Wickr ネットワークのデータ保持ボットを起動する
- Wickr ネットワークのデータ保持ボットを停止する

AWS Wickr のデータ保持を設定するための前提条件

開始する前に、Wickr AWS Management Console の からデータ保持ボット名 (ユーザー名) と初期パ スワードを取得する必要があります。データ保持ボットを初めて起動するときは、これらの値の両方 を指定する必要があります。また、コンソールでデータ保持を有効にする必要があります。詳細につ いては、「AWS Wickr でデータ保持の詳細を表示する」を参照してください。

AWS Wickr のデータ保持ボットのパスワード

データ保持ボットを初めて起動するときは、次のいずれかのオプションを使用して初期パスワードを 指定します。

- WICKRIO_BOT_PASSWORD 環境変数。データ保持ボットの環境変数については、<u>AWS Wickr で</u> データ保持ボットを設定する環境変数 本ガイドの後のセクションで概説しています。
- AWS_SECRET_NAME 環境変数によって識別される Secrets Manager の パスワード 値。データ保持 ボットの Secrets Manager の値については、<u>AWS Wickr の Secrets Manager 値</u> このガイドの後の セクションで概説されています。
- データ保持ボットのプロンプトが表示されたら、パスワードを入力します。-tiオプションを使用してインタラクティブな TTY アクセスでデータ保持ボットを実行する必要があります。

データ保持ボットを初めて設定すると、新しいパスワードが生成されます。データ保持ボットを再イ ンストールする必要がある場合は、生成されたパスワードを使用します。データ保持ボットを初めて インストールした後は、初期パスワードは無効になります。

新しく生成されたパスワードは、次の例のように表示されます。



パスワードを安全な場所に保存します。パスワードを紛失した場合、データ保持ボットを再 インストールすることはできません。このパスワードは共有しないでください。Wickr ネッ トワークのデータ保持を開始できるようになります。

**** GENERATED PASSWORD

- **** DO NOT LOSE THIS PASSWORD, YOU WILL NEED TO ENTER IT EVERY TIME
- **** TO START THE BOT
- "HuEXAMPLERAW41GgEXAMPLEn"

AWS Wickr ネットワークのストレージオプション

データ保持が有効になり、データ保持ボットが Wickr ネットワークに設定されると、ネットワーク 内で送信されるすべてのメッセージとファイルがキャプチャされます。メッセージは、環境変数を使 用して設定できる特定のサイズまたは時間制限に制限されたファイルに保存されます。詳細について は、「AWS Wickr でデータ保持ボットを設定する環境変数」を参照してください。

このデータを保存するには、次のオプションのいずれかを設定できます。

- キャプチャしたメッセージとファイルをすべてローカルに保存します。これがデフォルトのオプションです。ローカルファイルを別のシステムに移動して長期保存し、ホストディスクのメモリやスペースが不足しないようにするのはユーザーの責任です。
- キャプチャしたすべてのメッセージとファイルを Amazon S3 バケットに格納します。データ保持 ボットは、復号されたすべてのメッセージとファイルを、指定した Amazon S3 バケットに保存し ます。キャプチャされたメッセージとファイルは、バケットに正常に保存されるとホストマシンか ら削除されます。
- キャプチャしたすべてのメッセージとファイルを Amazon S3 バケットに暗号化して保存します。 データ保持ボットは、キャプチャされたすべてのメッセージとファイルを指定したキーを使用して 再暗号化し、指定した Amazon S3 バケットに保存します。キャプチャされたメッセージとファイ ルは、再暗号化に成功してバケットに保存されると、ホストマシンから削除されます。メッセージ とファイルを復号化するにはソフトウェアが必要です。

データ保持ボットで使用する Amazon S3 バケットの作成の詳細については、「Amazon S3 ユー ザーガイド」の「<u>バケットの作成</u>」を参照してください。

AWS Wickr でデータ保持ボットを設定する環境変数

次の環境変数を使用して、データ保持ボットを構成できます。これらの環境変数は、データ保持ボットの Docker イメージを実行するときの -e オプションを使用して設定します。詳細については、 「Wickr ネットワークのデータ保持ボットを起動する」を参照してください。

Note

これらの環境変数は、特に指定がない限りオプションです。

以下の環境変数を使用して、データ保持ボットの認証情報を指定します。

- WICKRIO_BOT_NAME データ保持ボットの名前。この変数は、データ保持ボットの Docker イ メージを実行する場合に 必要 です。
- WICKRIO_BOT_PASSWORD データ保持ボットの初期パスワード。詳細については、「<u>AWS</u> <u>Wickr のデータ保持を設定するための前提条件</u>」を参照してください。この変数は、パスワードプ ロンプトでデータ保持ボットを起動する予定がない場合や、Secrets Manager を使用してデータ保 持ボットの認証情報を保存する予定がない場合に 必要 です。

次の環境変数を使用して、デフォルトのデータ保持ストリーミング機能を設定します。

- WICKRIO_COMP_MESGDEST メッセージがストリーミングされるディレクトリへのパス名。デ フォルト値は /tmp/<botname>/compliance/messages です。
- WICKRIO_COMP_FILEDEST ファイルがストリーミングされるディレクトリへのパス名。デ フォルト値は /tmp/<botname>/compliance/attachments です。
- WICKRIO_COMP_BASENAME 受信したメッセージファイルのベース名。デフォルト値は receivedMessagesです。
- ・ WICKRIO_COMP_FILESIZE 受信メッセージファイルの最大ファイルサイズ (KiB)。最大サイズ に達すると、新しいファイルが開始されます。デフォルト値は 1000000000 (1024 GiB など) で す。
- WICKRIO_COMP_TIMEROTATE データ保持ボットが受信したメッセージを受信メッセージファ イルに保存する時間 (分単位)。制限時間に達すると、新しいファイルが開始されます。受信メッ セージファイルのサイズを制限できるのは、ファイルサイズまたは時間だけです。デフォルト値は 0 (制限なし)です。

次の環境変数を使用して、 AWS リージョン 使用するデフォルトを定義します。

AWS_DEFAULT_REGION – Secrets Manager などの AWS サービス AWS リージョン に使用するデフォルト (Amazon S3 や では使用されません AWS KMS)。この環境変数が定義されていない場合、デフォルトでは us-east-1 リージョンが使用されます。

次の環境変数を使用して、Secrets Manager を使用してデータ保持ボットの認証情報と AWS サービ ス情報を保存するときに使用する Secrets Manager シークレットを指定します。Secrets Manager に保存できる値の詳細については、AWS Wickr の Secrets Manager 値 を参照してください。

- AWS_SECRET_NAME データ保持ボットに必要な認証情報と AWS サービス情報を含む Secrets Manager シークレットの名前。
- AWS_SECRET_REGION AWS シークレット AWS リージョン が配置されている。 AWS シークレットを使用していて、この値が定義されていない場合は、 AWS_DEFAULT_REGION値が使用されます。

(i) Note

以下の環境変数はすべて、Secrets Manager に値として保存できます。Secrets Manager を 使用してこれらの値をそこに保存する場合、データ保持ボットの Dockerイメージを実行す るときに、それらを環境変数として指定する必要はありません。指定する必要があるのは、 このガイドで前述した AWS_SECRET_NAME 環境変数だけです。詳細については、「<u>AWS</u> Wickr の Secrets Manager 値」を参照してください。

メッセージとファイルをバケットに保存する場合は、以下の環境変数を使用して Amazon S3 バケッ トを指定します。

- ・ WICKRI0_S3_BUCKET_NAME— メッセージとファイルが保存される Amazon S3 バケットの名前。
- ・WICKRI0_S3_REGION メッセージとファイルが保存される Amazon S3 バケットの AWS リー ジョン。
- WICKRI0_S3_FOLDER_NAME— メッセージとファイルが保存される Amazon S3 バケットのオプ ションのフォルダ名。このフォルダ名の前には、Amazon S3 バケットに保存されるメッセージと ファイルのキーが先頭に付けられます。

クライアント側の暗号化を使用して Amazon S3 バケットに保存するときにファイルを再暗号化する 場合は、次の環境変数を使用して AWS KMS 詳細を指定します。

- WICKRIO_KMS_MSTRKEY_ARN Amazon S3 バケットに保存される前に、データ保持ボット上のメッセージファイルとファイルを再暗号化するために使用される AWS KMS マスターキーの Amazon リソースネーム (ARN)。 Amazon S3
- ・ WICKRIO_KMS_REGION マスターキーが AWS KMS 配置されている AWS リージョン。

Amazon SNS トピックにデータ保持イベントを送信することを選択した場合、次の環境変数を使用 して Amazon SNS の詳細を指定します。送信されるイベントには、スタートアップ、シャットダウ ン、エラー状態が含まれます。

• WICKRIO_SNS_TOPIC_ARN— データ保持イベントの送信先の Amazon SNS トピックの ARN。

次の環境変数を使用して、データ保持メトリクスを CloudWatch に送信します。指定した場合、メト リクスは 60 秒ごとに生成されます。

 WICKRI0_METRICS_TYPE— CloudWatch にメトリクスを送信するには、この環境変数の値を cloudwatch に設定します。

AWS Wickr の Secrets Manager 値

Secrets Manager を使用して、データ保持ボットの認証情報と AWS サービス情報を保存できま す。Secrets Manager シークレットの作成の詳細については、「 Secrets Manager <u>ユーザーガイ</u> <u>ド」の「 AWS Secrets Manager</u>シークレットの作成」を参照してください。

Secrets Manager のシークレットには、次の値を含めることができます。

- password— データ保持ボットのパスワード。
- s3_bucket_name— メッセージとファイルが保存される Amazon S3 バケットの名前。設定しない場合、デフォルトのファイルストリーミングが使用されます。
- ・ s3_region メッセージとファイルが保存される Amazon S3 バケットの AWS リージョン。
- s3_folder_name— メッセージとファイルが保存される Amazon S3 バケットのオプションの フォルダ名。このフォルダ名の前には、Amazon S3 バケットに保存されるメッセージとファイル のキーが先頭に付けられます。
- kms_master_key_arn Amazon S3 バケットに保存される前に、データ保持ボット上のメッセージファイルとファイルを再暗号化するために使用される AWS KMS マスターキーの ARN。
- ・ kms_region AWS KMS マスターキーが配置されている AWS リージョン。
- sns_topic_arn— データ保持イベントの送信先の Amazon SNS トピックの ARN。

AWS サービスでデータ保持を使用するための IAM ポリシー

Wickr データ保持ボットで他の AWS サービスを使用する場合は、ホストがそれらにアクセスするための適切な AWS Identity and Access Management (IAM) ロールとポリシーを持っていることを確認

する必要があります。Secrets Manager、Amazon S3、CloudWatch、Amazon SNS、および を使用 するようにデータ保持ボットを設定できます AWS KMS。次の IAM ポリシーでは、これらのサービ スの特定のアクションへのアクセスを許可します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                 "s3:PutObject",
                 "secretsmanager:GetSecretValue",
                "sns:Publish",
                "cloudwatch:PutMetricData",
                "kms:GenerateDataKey"
            ],
            "Resource": "*"
        }
    ]
}
```

ホスト上のコンテナにアクセスを許可したい各サービスの特定のオブジェクトを指 定することで、より厳密な IAM ポリシーを作成できます。使用しない AWS サービ スのアクションを削除します。たとえば、Amazon S3 バケットのみを使用する場合 は、、secretsmanager:GetSecretValue、sns:Publish、kms:GenerateDataKey、および cloudwatch:PutMetricData アクションを削除する次のポリシーを使用してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "*"
        }
    ]
}
```

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを使用してデータ保持ボットをホスト する場合は、Amazon EC2 の一般的なケースを使用して IAM ロールを作成し、上記のポリシー定義 を使用してポリシーを割り当てます。

Wickr ネットワークのデータ保持ボットを起動する

データ保持ボットを実行する前に、その設定方法を決定する必要があります。次のようなホストで ボットを稼働させる予定がある場合

- AWS サービスにはアクセスできないため、オプションは限られています。その場合は、デフォルトのメッセージストリーミングオプションを使用します。キャプチャするメッセージファイルのサイズを特定のサイズに制限するか、時間間隔に制限するかを決定する必要があります。詳細については、「AWS Wickr でデータ保持ボットを設定する環境変数」を参照してください。
- AWS サービスにアクセスできるため、Secrets Manager シークレットを作成して、ボットの認証 情報と AWS サービス設定の詳細を保存する必要があります。 AWS サービスを設定したら、デー タ保持ボットの Dockerイメージを起動できます。Secrets Manager シークレットに保存できる詳 細についての詳細は、AWS Wickr の Secrets Manager 値 を参照してください。

以下のセクションでは、データ保持ボットの Docker イメージを実行するコマンドの例を示します。 各コマンド例で、次の例の値を独自の値に置き換えます。

- compliance_1234567890_bot をデータ保持ボットの名前に置き換えます。
- password にデータ保持ボットのパスワードを入力します。
- wickr/data/retention/bot にデータ保持ボットで使用する Secrets Manager シークレットの 名前を付けます。
- bucket-name にメッセージとファイルが保存される Amazon S3 バケットの名前を指定します。
- folder-name にメッセージとファイルが保存される Amazon S3 バケット内のフォルダ名を指定 します。
- us-east-1は、指定するリソースのAWSリージョンに置き換えます。例えば、AWSKMSマスターキーのリージョンやAmazonS3バケットのリージョンなどです。
- arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617ababababababab メッセージファイルとファイルの再暗号化に使用する AWS KMS マスターキーの Amazon リソースネーム (ARN) を持つ。

パスワード環境変数を使用してボットを起動する(AWS サービスなし)

次の Docker コマンドはデータ保持ボットを起動します。パスワードは WICKRIO_BOT_PASSWORD 環境変数を使用して指定されます。ボットは、デフォルトのファイルストリーミングと、このガイド の <u>AWS Wickr でデータ保持ボットを設定する環境変数</u> セクションで定義されているデフォルト値の 使用を開始します。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRI0_BOT_NAME='compliance_1234567890_bot' \
-e WICKRI0_BOT_PASSWORD='password' \
wickr/bot-compliance-cloud:latest
```

パスワードプロンプトでボットを起動する(AWS サービスなし)

次の Docker コマンドはデータ保持ボットを起動します。パスワードは、データ保持ボットによって 要求されたときに入力されます。このガイドの <u>AWS Wickr でデータ保持ボットを設定する環境変数</u> セクションで定義されているデフォルト値を使用して、デフォルトのファイルストリーミングを開始 します。

パスワードプロンプトを受け取る -ti オプションを使用してボットを実行します。また、docker イ メージを起動した直後に docker attach *<container ID or container name>* コマンドを 実行して、パスワードプロンプトが表示されるようにする必要があります。これらのコマンドは両方 ともスクリプトで実行する必要があります。Docker イメージにアタッチしてもプロンプトが表示さ れない場合は、Enter キーを押すとプロンプトが表示されます。 15 分間のメッセージファイルのローテーションでボットを開始する (AWS サービスなし)

次の Docker コマンドは、環境変数を使用してデータ保持ボットを起動します。また、受信したメッ セージファイルを 15 分にローテーションするように設定しています。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_COMP_TIMEROTATE=15 \
wickr/bot-compliance-cloud:latest
```

ボットを起動し、Secrets Manager で初期パスワードを指定する

Secrets Manager を使用して、データ保持ボットのパスワードを特定できます。データ保持ボットを 起動するときは、この情報を保存する Secrets Manager を指定する環境変数を設定する必要があり ます。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e AWS_SECRET_NAME='wickrpro/alpha/new-3-bot' \
wickr/bot-compliance-cloud:latest
```

wickrpro/compliance/compliance_1234567890_bot シークレットには以下のシークレット 値があり、プレーンテキストで表示されます。



ボットを起動し、Secrets Manager で Amazon S3 を設定する

Secrets Manager を使用して、認証情報と Amazon S3 バケット情報をホストできます。データ保持 ボットを起動するときは、この情報を保存する Secrets Manager を指定する環境変数を設定する必 要があります。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
```

```
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
    -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
    -e AWS_SECRET_NAME='wickrpro/alpha/compliance_1234567890_bot' \
wickr/bot-compliance-cloud:latest
```

wickrpro/compliance/compliance_1234567890_bot シークレットには以下のシークレット 値があり、プレーンテキストで表示されます。

```
{
    "password":"password",
    "s3_bucket_name":"bucket-name",
    "s3_region":"us-east-1",
    "s3_folder_name":"folder-name"
}
```

ボットが受信したメッセージとファイルは、network1234567890 という名前のフォルダー内の bot-compliance バケットに格納されます。

Secrets Manager AWS KMS を使用してボットを起動し、Amazon S3 と を設定する

Secrets Manager を使用して、認証情報、Amazon S3 バケット、 AWS KMS マスターキー情報をホ ストできます。データ保持ボットを起動するときは、この情報を保存する Secrets Manager を指定 する環境変数を設定する必要があります。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRI0_BOT_NAME='compliance_1234567890_bot' \
-e AWS_SECRET_NAME='wickrpro/alpha/compliance_1234567890_bot' \
wickr/bot-compliance-cloud:latest
```

wickrpro/compliance/compliance_1234567890_bot シークレットには以下のシークレット 値があり、プレーンテキストで表示されます。

```
{
    "password":"password",
    "s3_bucket_name":"bucket-name",
    "s3_region":"us-east-1",
    "s3_folder_name":"folder-name",
    "kms_master_key_arn":"arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-
a617-abababababab",
    "kms_region":"us-east-1"
```

}

ボットが受信したメッセージとファイルは、ARN 値で識別される KMS キーを使用して暗号化さ れ、「network1234567890」という名前のフォルダーの「bot-compliance」バケットに格納されま す。適切な IAM ポリシーが設定されていることを確認します。

ボットを起動し、環境変数を使用して Amazon S3 を設定する

Secrets Manager を使用してデータ保持ボットの認証情報をホストしたくない場合は、以下の環境変数を使用してデータ保持ボットの Dockerイメージを起動できます。WICKRIO_BOT_NAME 環境変数を使用してデータ保持ボットの名前を特定する必要があります。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRI0_BOT_NAME='compliance_1234567890_bot' \
-e WICKRI0_BOT_PASSWORD='password' \
-e WICKRI0_S3_BUCKET_NAME='bot-compliance' \
-e WICKRI0_S3_FOLDER_NAME='network1234567890' \
-e WICKRI0_S3_REGION='us-east-1' \
wickr/bot-compliance-cloud:latest
```

環境値を使用して、データ保持ボットの認証情報、Amazon S3 バケットに関する情報、およびデ フォルトのファイルストリーミングの設定情報を識別できます。

Wickr ネットワークのデータ保持ボットを停止する

データ保持ボットで実行されているソフトウェアが SIGTERM 信号をキャプチャし、正常にシャット ダウンします。以下の例に示すように docker stop *<container ID or container name>* コ マンドを使用して、データ保持ボットのDockerイメージに SIGTERM コマンドを実行します。

docker stop compliance_1234567890_bot

Wickr ネットワークのデータ保持ログを取得する

データ保持ボットの Docker イメージで実行されているソフトウェアは、/tmp/*<botname>/*logs ディレクトリ内のログファイルに出力されます。最大 5 つのファイルにローテーションされます。 以下のコマンドを実行すれば、ログを取得できる。

```
docker logs <botname>
```

例:

docker logs compliance_1234567890_bot

Wickr ネットワークのデータ保持メトリクスとイベント

以下は、AWS Wickr データ保持ボットの 5.116 バージョンで現在サポートされている Amazon CloudWatch (CloudWatch) メトリックスと Amazon Simple Notification Service (Amazon SNS) イベ ントです。

トピック

- Wickr ネットワークの CloudWatch メトリクス
- Wickr ネットワークの Amazon SNS イベント

Wickr ネットワークの CloudWatch メトリクス

メトリクスは1分間隔でボットによって生成され、データ保持ボットの Docker イメージが実行され ているアカウントに関連付けられた CloudWatch サービスに送信されます。

データ保持ボットがサポートする既存のメトリックスは次のとおりです。

メトリクス	説明
Messages_Rx	メッセージを受信しました。
Messages_Rx_Failed	受信したメッセージを処理できませんでした。
Messages_Saved	メッセージは受信メッセージファイルに保存さ れます。
Messages_Saved_Failed	受信メッセージファイルへのメッセージの保存 に失敗しました。
Files_Saved	ファイルを受信しました。
Files_Saved_Bytes	受信したファイルのバイト数。
Files_Saved_Failed	ファイルの保存に失敗しました。

メトリクス	説明
ログイン	ログイン(通常、各ログイン間隔で1回で す)。
Login_Failures	ログインに失敗した(通常、各ログイン間隔で 1 回です)。
S3_Post_Errors	メッセージファイルおよびファイルを Amazon S3 バケットに送信中にエラーが発生しまし た。
Watchdog_Failures	ウォッチドッグの障害。
Watchdog_Warnings	ウォッチドッグの警告。

メトリックスは CloudWatch によって消費されるように生成されます。ボットに使用される名前空間 は WickrIO です。各メトリクスにはディメンションの配列があります。以下は、上記のメトリクス とともに掲載されるディメンションのリストです。

ディメンション	值
ID	ボットのユーザー名。
デバイス	特定のボットデバイスまたはインスタンスの説 明。複数のボットデバイスまたはインスタンス を実行している場合に便利です。
製品	ボット用の製品。Alpha、Beta、または Production を付加したWickrPro_ また はWickrEnterprise_ にすることができま す。
BotType	ボットタイプ。コンプライアンスボットには コンプライアンス というラベルが付けられま す。
ネットワーク	関連付けられたネットワークの ID。

Wickr ネットワークの Amazon SNS イベント

以下のイベントは、WICKRIO_SNS_TOPIC_ARN 環境変数または sns_topic_arn Secrets Manager のシークレット値を使用して識別される Amazon リソースネーム (ARN) 値によって定義された Amazon SNS トピックに投稿されます。詳細については、「<u>AWS Wickr でデータ保持ボットを設定</u> する環境変数」および「AWS Wickr の Secrets Manager 値」を参照してください。

データ保持ボットによって生成されたイベントは JSON 文字列として送信されます。データ保持 ボットの 5.116 バージョンでは、以下の値がイベントに含まれています。

名前	值
complianceBot	データ保持ボットのユーザー名。
dataTime	イベントが発生したときの日時
デバイス	特定のボットデバイスまたはインスタンスの説 明。複数のボットインスタンスを実行している 場合に便利です。
dockerImage	ボットに関連付けられている Docker イメー ジ。
dockerTag	Docker イメージのタグまたはバージョン。
message	イベントメッセージ。詳細については、「 <u>重要</u> <u>なイベント</u> 」および「 <u>通常のイベント</u> 」を参照 してください。
notificationType	この値は Bot Event になります。
severity	イベントの重要度。normal または critical のいずれかを設定できます。

イベントを受信するには、Amazon SNS トピックにサブスクライブする必要があります。E メール アドレスを使用してサブスクライブすると、次の例のような情報を含む E メールが送信されます。

"complianceBot": "compliance_1234567890_bot",

{

```
"dateTime": "2022-10-12T13:05:39",
"device": "Desktop 1234567890ab",
"dockerImage": "wickr/bot-compliance-cloud",
"dockerTag": "5.116.13.01",
"message": "Logged in",
"notificationType": "Bot Event",
"severity": "normal"
}
```

重要なイベント

これらのイベントにより、ボットは停止または再起動します。他の問題を引き起こさないように、再 起動の回数は制限されています。

ログイン失敗

ボットがログインに失敗した場合に発生する可能性のあるイベントは次のとおりです。各メッセージ には、ログインに失敗した理由が示されます。

イベントタイプ	イベントメッセージ
failedlogin	不正な認証情報。パスワードを確認してくださ い。
failedlogin	ユーザーが見つかりません。
failedlogin	アカウントまたはデバイスが停止されていま す。
プロビジョニング	ユーザーはコマンドを終了した。
プロビジョニング	config.wickr ファイルのパスワードが不正 です。
プロビジョニング	config.wickr ファイルを読み込めません。
failedlogin	ログインがすべて失敗しました。
failedlogin	新しいユーザーですが、データベースはすでに 存在しています。

より重大なイベント

イベントタイプ	イベントメッセージ
停止中のアカウント	WickrIOClientMain::slotAdminUserSuspend: code(%1): reason: %2"
BotDevice Suspended	デバイスが停止されました。
ウォッチドッグ	スイッチボードシステムが <n> 分以上停止し ています</n>
S3 障害	ファイル < <i>file-name</i> ≫ を S3 バケットに配 置できませんでした。エラー: < <i>AWS-error</i> >
フォールバックキー	SERVER SUBMIITED FALLBACK KEY: クライ アント側で認識されているアクティブなフォー ルバックキーではありません。デスクトップエ ンジニアリングにログを送信してください。

通常のイベント

通常の運用状況について警告するイベントは次のとおりです。特定の期間内にこの種のイベントが多 発すると、懸念の原因となることがあります。

デバイスがアカウントに追加されました

このイベントは、データ保持ボットアカウントに新しいデバイスが追加されたときに生成されます。 状況によっては、これは誰かがデータ保持ボットのインスタンスを作成したことを示す重要な指標と なることがあります。以下は、このイベントのメッセージです。

A device has been added to this account!

Bot がログインしました

このイベントは、ボットが正常にログインしたときに生成されます。以下は、このイベントのメッ セージです。

Logged in

シャットダウン

このイベントは、ボットのシャットダウン時に生成されます。ユーザーがこれを明示的に開始しな かった場合、問題が発生している可能性があります。以下は、このイベントのメッセージです。

Shutting down

更新があります

{

このイベントは、データ保持ボットが起動し、関連する Docker イメージの新しいバージョンが使用 可能であることが確認されたときに生成されます。このイベントは、ボットの起動時に毎日生成され ます。このイベントには、利用可能な新しいバージョンを識別する versions 配列フィールドが含 まれます。以下に示しているのは、イベントの具体的な例です。

```
"complianceBot": "compliance_1234567890_bot",
"dateTime": "2022-10-12T13:05:55",
"device": "Desktop 1234567890ab",
"dockerImage": "wickr/bot-compliance-cloud",
"dockerTag": "5.116.13.01",
"message": "There are updates available",
"notificationType": "Bot Event",
"severity": "normal",
"versions": [
    "5.116.10.01"
]
}
```

ATAK とは

Android チーム認識キット (ATAK) は、軍事用 Android タクティカルアサルトキット (同じく ATAK) とも呼ばれるスマートフォンでの地理空間インフラストラクチャおよび状況認識アプリケーションで あり、地理的に離れた場所での安全なコラボレーションを可能にします。ATAK は当初、戦闘地帯で の使用を想定して設計されていましたが、地方、州、および連邦機関の任務に合うように適合されて います。

トピック

- Wickr ネットワークダッシュボードで ATAK を有効にする
- ATAK に関する追加情報

- ATAK 用 Wickr プラグインをインストールしてペアリングする
- ATAK 用の Wickr プラグインのペアリングを解除する
- ATAK でダイヤルして通話を受信する
- ATAK でファイルを送信する
- ATAK で安全な音声メッセージ (Push-to-talk) を送信する
- ATAK のピンホイール (クイックアクセス)
- ATAK のナビゲーション

Wickr ネットワークダッシュボードで ATAK を有効にする

AWS Wickr は Android Tactical Assault Kit (ATAK) を使用する多くの機関をサポートしています。た だし、これまで Wickr を使用する ATAK オペレーターは、そのためにはアプリケーションを終了す る必要がありました。中断と運用リスクを軽減するために、Wickr は ATAK を安全な通信機能で強化 するプラグインを開発しました。ATAK 用 Wickr プラグインを使用すると、ユーザーは ATAK アプ リケーション内で Wickr 上でメッセージを送ったり、共同作業を行ったり、ファイルを転送したり できます。これにより、中断がなくなり、ATAK のチャット機能の設定が複雑になることもなくなり ます。

Wickr ネットワークダッシュボードで ATAK を有効にする

Wickr ネットワークダッシュボードで ATAK を有効にするには、以下の手順を実行します。

- 1. Wickr AWS Management Console の を <u>https://console.aws.amazon.com/wickr/</u>://https//https//ht
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、[Security Groups] (セキュリティグループ) を選択します。
- 4. セキュリティグループページで、ATAK を有効にするセキュリティグループを選択します。
- 5. 統合タブの ATAK プラグインセクションで、編集を選択します。
- 6. ATAK プラグインの編集ページで、ATAK プラグインを有効にするチェックボックスをオンにし ます。
- 7. 新しいパッケージの追加を選択する
- 8. パッケージ テキストボックスにパッケージ名を入力します。ユーザーがインストールおよび使 用する ATAK のバージョンに応じて、次のいずれかの値を入力できます。

- com.atakmap.app.civ—Wickr エンドユーザーが Android デバイスに民間版の ATAK アプ リケーションをインストールして使用する場合は、この値を「パッケージ」テキストボックス に入力します。
- com.atakmap.app.mi1— Wickr エンドユーザーが Android デバイスに軍用バージョンの ATAK アプリケーションをインストールして使用する場合は、この値を「パッケージ」テキス トボックスに入力します。
- 9. [保存]を選択します。

これで、選択した Wickr ネットワークと選択したセキュリティグループで ATAK が有効になり ました。ATAK 機能を有効にしたセキュリティグループの Android ユーザーに、ATAK 用 Wickr プラグインをインストールするよう依頼してください。詳細については、「<u>Wickr ATAK プラグ</u> インのインストールとペア」を参照してください。

ATAK に関する追加情報

ATAK 用 Wickr プラグインの詳細については、以下を参照してください。

- Wickr ATAK プラグインの概要
- Wickr ATAK プラグイン追加情報

ATAK 用 Wickr プラグインをインストールしてペアリングする

Android チーム認識キット (ATAK) は、ミッションの計画、実行、インシデント対応に状況認識機能 を必要とする米軍、州、政府機関で使用されている Android ソリューションです。ATAK には、開 発者が機能を追加できるプラグインアーキテクチャがあります。これにより、ユーザーは GPS と 地理空間マップデータと、進行中のイベントのリアルタイムの状況認識を組み合わせてナビゲート できます。このドキュメントでは、Android デバイスに ATAK 用 Wickr プラグインをインストール し、Wickr クライアントとペアリングする方法を説明します。これにより、ATAK アプリケーション を終了しなくても Wickr でメッセージを送ったり、共同作業を行ったりできます。

ATAK用のWickrプラグインをインストールします。

Android デバイスに ATAK 用 Wickr プラグインをインストールするには、次の手順を実行します。

1. Google Play ストアに移動し、ATAK 用 Wickr プラグインをインストールしてください。

)

- 2. Android デバイスで ATAK アプリケーションを開きます。
- 3. ATAK アプリケーションで、画面の右上にあるメニューアイコン

を選択し、[プラグイン]を選択します。

- 4. [インポート]を選択します。
- 5. [インポートタイプの選択] ポップアップで [ローカル SD] を選択し、ATAK 用 Wickr プラグイ ン .apk ファイルを保存した場所に移動します。
- 6. プラグインファイルを選択し、インストールするための指示に従います。

(i) Note スキャン用にプラグインファイルを送信するように求められた場合は、いいえ を選択し ます。

 ATAK アプリケーションから、プラグインをロードするかどうかを尋ねます。[OK] を選択して ください。

ATAK 用の Wickr プラグインがインストールされました。次の「ATAK と Wickr のペアリング」セク ションに進んでプロセスを終了してください。

ATAK と Wickr のペアリング

ATAK 用 Wickr プラグインが正常にインストールされたら、次の手順を実行して ATAK アプリケー ションと Wickr をペアリングします。

1. ATAK アプリケーションで、画面の右上にあるメニューアイコン

を選択し、次に [Wickr プラグイン] を選択します。

2. [Wickr とペアリング]を選択します。

ATAK 用 Wickr プラグインのアクセス許可を確認するように求める通知プロンプトが表示され ます。通知プロンプトが表示されない場合は、Wickr クライアントを開いて [設定]、[接続アプリ ケーション] の順に移動します。画面の [保留中] セクションにプラグインが表示されます。

- 3. [承認]を選択してペアリングします。
- 4. [Wickr ATAK プラグインを開く] ボタンを選択して ATAK アプリケーションに戻ります。

)

これで ATAK プラグインと Wickr のペアリングが完了しました。ATAK アプリケーションを終 了しなくても、プラグインを使用してメッセージを送信したり、Wickr を使用して共同作業を 行ったりできます。

ATAK 用の Wickr プラグインのペアリングを解除する

ATAK 用の Wickr プラグインのペアリングを解除できます。

ATAK プラグインと Wickr のペアリングを解除するには、次の手順を実行します。

- 1. ネイティブアプリで、[設定]、[接続アプリケーション]の順に選択します。
- 2. [接続アプリケーション] 画面で、[Wickr ATAK プラグイン] を選択します。
- 3. [Wickr ATAK プラグイン] 画面で、画面下部の [削除] を選択します。

これで、ATAK 用の Wickr プラグインのペアリングが正常に解除されました。

ATAK でダイヤルして通話を受信する

ATAK 用 Wickr プラグインではダイヤル発信と着信を行うことができます。

ダイヤル発信と着信を行うには、次の手順を実行します。

- 1. チャットウィンドウを開きます。
- 2. [マップ] ビューで、電話をかけるユーザーのアイコンを選択します。
- 3. 画面の右上にある電話アイコンを選択します。
- 4. 接続したら、ATAK プラグインビューに戻って電話を受けることができます。

ATAK でファイルを送信する

ATAK 用 Wickr プラグインでファイルを送信できます。

ファイルを送信するには、次の手順を実行します。

- 1. チャットウィンドウを開きます。
- 2. [マップ] ビューで、ファイルを送信するユーザーを検索します。
- 3. ファイルを送信するユーザーを見つけたら、その名前を選択します。

4. [ファイルの送信] 画面で [ファイルの選択] を選択し、送信するファイルに移動します。

	223 · 223		≅ ⊕ ≋
MASHINGTON MONTANA CERT IDAHO RETORY	NORTH DAKOTA	Send File	
NEVADA UTAH	G NEBRASKA Denver	file name.PDF	
D ALIFORNIA Los Angeles ARIZON A NEW	MEXICO	Choose	File
Phoenix 1,099 km	SIT(X) – TAK – WICK Callsign: BACKY 14R PU 10708 79232 1,009 ft MSL 171°M 0 MPH +/- 4m	Send File	Cancel

- 5. ブラウザウィンドウで、目的のファイルを選択します。
- 6. [ファイルの送信] 画面で、[ファイルの送信] を選択します。

選択したファイルがダウンロード中であることを示すダウンロードアイコンが表示されます。

ATAK で安全な音声メッセージ (Push-to-talk) を送信する

ATAK 用 Wickr プラグインで安全な音声メッセージを送信できます (プッシュトゥトーク)。

安全な音声メッセージを送信するには、次の手順を実行します。

- 1. チャットウィンドウを開きます。
- 画面上部の [プッシュトゥトーク] アイコンを選択します。これは会話している人のアイコンで 示されます。



3. [長押しして録音] ボタンを選択し、長押しします。



- 4. メッセージを録音します。
- 5. メッセージを録音した後、ボタンを離すと送信されます。

ATAK のピンホイール (クイックアクセス)

ピンホイール、別名クイックアクセス機能は、1 対 1 の会話やダイレクトメッセージに使用されま す。

ピンホイールを使用するには、次の手順を実行します。

- 1. ATAK マップの分割画面ビューと ATAK 用 Wickr プラグインを同時に開きます。マップには チームメイトやアセットがマップビュー上に表示されます。
- 2. ユーザーアイコンを選択すると、ピンホイールが開きます。
- 3. Wickr アイコンを選択すると、選択したユーザーが利用できるオプションが表示されます。



4. ピンホイールで、以下のいずれかのアイコンを選択します。

• [電話]: 電話をかける場合に選択します。



• [メッセージ]: チャットする場合に選択します。



• [ファイル送信]: ファイルを送信する場合に選択します。



ATAK のナビゲーション

プラグイン UI には、画面の右下にある青と白の図形で示される 3 つのプラグインビューがありま す。ビュー間を移動するには左右にスワイプします。

- [連絡先ビュー]: ダイレクトメッセージグループまたは会話ルームを作成します。
- [DM ビュー]: 1 対 1 の会話を作成します。チャット機能は Wickr のネイティブアプリと同様に機能 します。この機能により、マップビューを開いたまま、プラグイン上で他のユーザーと通信できま す。
- [ルームビュー]: ネイティブアプリ内の既存のルームが移植されます。プラグインでの操作はすべて Wickr ネイティブアプリに反映されます。

Note

ルームの削除などの特定の機能は、ユーザーによる意図しない変更や現場の機器による干 渉を防ぐために、ネイティブアプリで直接行う場合のみ実行できます。

Wickr ネットワークのリストを許可するポートとドメイン

Wickr が正しく機能するように、次のポートのリストを許可します。

ポート

- TCP ポート 443 (メッセージと添付ファイル用)
- ・ UDP ポート 16384-16584(通話用)

リージョン別の許可リストのドメインとアドレス

可能なすべての呼び出しドメインとサーバー IP アドレスを許可リストに登録する必要がある場合 は、リージョン別の潜在的な CIDRs の次のリストを参照してください。このリストは変更される可 能性があるため、定期的に確認してください。

Note

登録 E メールと確認 E メールは donotreply@wickr.email から送信されます。

米国東部 (バージニア北部)

ドメイン :	 gw-pro-prod.wickr.com api.messaging.wickr.us-east-1.amazon aws.com
CIDR アドレスの呼び出し:	44.211.195.0/2744.213.83.32/28
IP アドレスの呼び出し:	 44.211.195.0 44.211.195.1 44.211.195.2 44.211.195.3 44.211.195.4 44.211.195.5 44.211.195.6

- 44.211.195.7
- 44.211.195.8
- 44.211.195.9
- 44.211.195.10
- 44.211.195.11
- 44.211.195.12
- 44.211.195.13
- 44.211.195.14
- 44.211.195.15
- 44.211.195.16
- 44.211.195.17
- 44.211.195.18
- 44.211.195.19
- 44.211.195.20
- 44.211.195.21
- 44.211.195.22
- 44.211.195.23
- 44.211.195.24
- 44.211.195.25
- 44.211.195.26
- 44.211.195.27
- 44.211.195.28
- 44.211.195.29
- 44.211.195.30
- 44.211.195.31
- 44.213.83.32
- 44.213.83.33
- 44.213.83.34
- 44.213.83.35
- 44.213.83.36

- 44.213.83.37
- 44.213.83.38
- 44.213.83.39
- 44.213.83.40
- 44.213.83.41
- 44.213.83.42
- 44.213.83.43
- 44.213.83.44
- 44.213.83.45
- 44.213.83.46
- 44.213.83.47

アジアパシフィック (マレーシア)

ドメイン:	 gw-pro-prod.wickr.com
	 api.messaging.wickr.ap-southeast-5.a mazonaws.com
CIDR アドレスの呼び出し:	• 43.216.226.160/28
IP アドレスの呼び出し:	• 43.216.226.160
	• 43.216.226.161
	• 43.216.226.162
	• 43.216.226.163
	• 43.216.226.164
	• 43.216.226.165
	• 43.216.226.166
	• 43.216.226.167
	• 43.216.226.168
	• 43.216.226.169
	• 43.216.226.170
	• 43.216.226.171

•	43.216.226.172

- 43.216.226.173
- 43.216.226.174
- 43.216.226.175

アジアパシフィック (シンガポール)

ドメイン:	 gw-pro-prod.wickr.com api.messaging.wickr.ap-southeast-1.a mazonaws.com
CIDR アドレスの呼び出し:	• 47.129.23.144/28
IP アドレスの呼び出し :	 47.129.23.144 47.129.23.145 47.129.23.146 47.129.23.147 47.129.23.148 47.129.23.149 47.129.23.150 47.129.23.151 47.129.23.152 47.129.23.153 47.129.23.154 47.129.23.155 47.129.23.156 47.129.23.157 47.129.23.158 47.129.23.159

アジアパシフィック (シドニー)	
ドメイン :	 gw-pro-prod.wickr.com api.messaging.wickr.ap-southeast-2.a mazonaws.com
CIDR アドレスの呼び出し:	• 3.27.180.208/28
IP アドレスの呼び出し :	 3.27.180.208 3.27.180.209 3.27.180.210 3.27.180.211 3.27.180.212 3.27.180.213 3.27.180.214 3.27.180.215 3.27.180.216 3.27.180.217 3.27.180.218 3.27.180.219 3.27.180.220 3.27.180.221 3.27.180.222 3.27.180.223

アジアパシフィック (東京)

ドメイン :	 gw-pro-prod.wickr.com api.messaging.wickr.ap-northeast-1.a mazonaws.com
CIDR アドレスの呼び出し:	• 57.181.142.240/28

IP アドレスの呼び出し:	• 57.181.142.240
	• 57.181.142.241
	• 57.181.142.242
	• 57.181.142.243
	• 57.181.142.244
	• 57.181.142.245
	• 57.181.142.246
	• 57.181.142.247
	• 57.181.142.248
	• 57.181.142.249
	• 57.181.142.250
	• 57.181.142.251
	• 57.181.142.252
	• 57.181.142.253
	• 57.181.142.254
	• 57.181.142.255
カナダ (中部)	
ドメイン:	 gw-pro-prod.wickr.com
	 api.messaging.wickr.ca-central-1.ama
	zonaws.com
CIDR アドレスの呼び出し:	• 15.156.152.96/28
IP アドレスの呼び出し:	• 15.156.152.96
	• 15.156.152.97
	• 15.156.152.98
	• 15.156.152.99
	• 15.156.152.100
	• 15.156.152.101
	• 15.156.152.102

	 15.156.152.103 15.156.152.104 15.156.152.105 15.156.152.106 15.156.152.107 15.156.152.108
	 15.156.152.109 15.156.152.110 15.156.152.111
欧州 (フランクフルト)	
ドメイン :	 gw-pro-prod.wickr.com api.messaging.wickr.eu-central-1.ama zonaws.com
CIDR アドレスの呼び出し:	• 3.78.252.32/28
IP アドレスの呼び出し :	 3.78.252.32 3.78.252.33 3.78.252.34 3.78.252.35 3.78.252.36 3.78.252.37 3.78.252.38 3.78.252.39 3.78.252.40 3.78.252.41 3.78.252.42 3.78.252.43 3.78.252.43 3.78.252.44 3.78.252.45

	3.78.252.463.78.252.47
メッセージング IP アドレス :	 3.78.252.47 3.163.236.183 3.163.238.183 3.163.251.183 3.163.232.183 3.163.241.183 3.163.245.183 3.163.245.183 3.163.248.183 3.163.237.183 3.163.247.183 3.163.247.183 3.163.240.183 3.163.242.183 3.163.244.183 3.163.244.183 3.163.249.183 3.163.249.183 3.163.252.183 3.163.235.183
	 3.163.250.183 3.163.239.183 3.163.233.183
	0.100.200.100

欧州 (ロンドン)

ドメイン:	 gw-pro-prod.wickr.com api.messaging.wickr.eu-west-2.amazon aws.com
CIDR アドレスの呼び出し:	• 13.43.91.48/28
IP アドレスの呼び出し:	• 13.43.91.48
-----------------	---
	• 13.43.91.49
	• 13.43.91.50
	• 13.43.91.51
	• 13.43.91.52
	• 13.43.91.53
	• 13.43.91.54
	• 13.43.91.55
	• 13.43.91.56
	• 13.43.91.57
	• 13.43.91.58
	• 13.43.91.59
	• 13.43.91.60
	• 13.43.91.61
	• 13.43.91.62
	• 13.43.91.63
欧州 (ストックホルム)	
ドメイン:	 gw-pro-prod.wickr.com
	 api.messaging.wickr.eu-north-1.amazo naws.com
CIDR アドレスの呼び出し:	• 13.60.1.64/28
IP アドレスの呼び出し:	• 13.60.1.64

• 13.60.1.65

• 13.60.1.66

• 13.60.1.67

• 13.60.1.68

• 13.60.1.69

• 13.60.1.70

13.60.1.	71
----------	----

• 13.60.1.72

• 13.60.1.73

• 13.60.1.74

• 13.60.1.75

• 13.60.1.76

• 13.60.1.77

• 13.60.1.78

• 13.60.1.79

欧州 (チューリッヒ)

ドメイン :	gw-pro-prod.wickr.comapi.messaging.wickr.eu-central-2.ama zonaws.com
CIDR アドレスの呼び出し:	• 16.63.106.224/28
IP アドレスの呼び出し :	 16.63.106.224 16.63.106.225 16.63.106.226 16.63.106.227 16.63.106.228 16.63.106.229 16.63.106.230 16.63.106.231 16.63.106.232 16.63.106.233 16.63.106.235 16.63.106.236 16.63.106.237

- 16.63.106.238
- 16.63.106.239

AWS GovCloud (米国西部)

ドメイン :	 gw-pro-prod.wickr.com api.messaging.wickr.us-gov-west-1.am azonaws.com
CIDR アドレスの呼び出し:	• 3.30.186.208/28
IP アドレスの呼び出し :	 3.30.186.208 3.30.186.209 3.30.186.210 3.30.186.211 3.30.186.212 3.30.186.213 3.30.186.214 3.30.186.215 3.30.186.216 3.30.186.217 3.30.186.218 3.30.186.219 3.30.186.220 3.30.186.221 3.30.186.221 3.30.186.222 3.30.186.223

GovCloud クロス境界分類とフェデレーション

AWS Wickr は、 GovCloud ユーザー向けにカスタマイズされた WickrGov クライアントを提供します。 GovCloud GovCloud フェデレーションを使用すると、 GovCloud ユーザーと商用ユーザー間の

通信が可能になります。クロス境界分類機能により、 GovCloud ユーザーの会話に対するユーザー インターフェイスの変更が可能になります。GovCloud ユーザーとして、政府定義の分類に関する 厳格なガイドラインに従う必要があります。GovCloud ユーザーが商用ユーザー (エンタープライ ズ、AWS Wickr、ゲストユーザー) と会話すると、次の分類されていない警告が表示されます。

- ルームリストの U タグ
- ・ メッセージ画面上の分類されていない確認
- 会話の上部にある分類されていないバナー

9:41		,ul 🗢 🖿
Edit	Rooms	Ľ
Q Sea	ırch	
PINNED		
	Finance Room Amanda: We want to thank for the hard work and effort	9:32 AM each of you you put
Q	Sandra Gill, Randall Mars Randall: Most of the notifica were for soccer teams I follo	h ^{Yesterday} ations ow.
ROOMS	Dev Team Weekly Joan: You may be aware tha	9:09 AM It email
	Product Room Lorem ipsum dolor sit amet consectetur adipiscing elit,	7/14/22 sed do.
A	Sales Approval	7/14/22
A	Lorem ipsum dolor sit amet consectetur adipiscing elit,	sed do.
	HR Announcement Lorem ipsum dolor sit amet consectetur adipiscing elit,	7/14/22 sed do.
Rooms	Direct Messages Contacts	ريَ Settings

Note

これらの警告は、 GovCloud ユーザーが外部ユーザーと会話しているとき、またはルームの 一部である場合にのみ表示されます。外部ユーザーが会話を終了すると、それらは消えま す。GovCloud ユーザー間の会話には警告は表示されません。

AWS Wickr のファイルプレビュー

Wickr Premium 階層 (Premium 無料トライアルを含む) を使用している組織は、セキュリティグルー プレベルでファイルのダウンロード許可を管理できるようになりました。

ファイルのダウンロードは、セキュリティグループでデフォルトで有効になっています。管理者は、 管理者パネルを使用してファイルのダウンロードを有効または無効にできます。この設定は Wickr ネットワーク全体に適用されます。

ファイルのダウンロードを有効または無効にするには、次の手順を実行します。

- 1. Wickr AWS Management Consoleのをhttps://console.aws.amazon.com/wickr/で開きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、[Security Groups] (セキュリティグループ) を選択します。
- 4. 編集するセキュリティグループの名前を選択します。

セキュリティグループの詳細ページには、セキュリティグループの設定がさまざまなタブに表示 されます。

- 5. メッセージングタブの「メディアとリンク」セクションで「編集」を選択します。
- メディアとリンクの編集ページで、ファイルのダウンロードオプションをオンまたはオフにします。
- 7. [Save changes] (変更の保存) をクリックします。

セキュリティグループでファイルのダウンロードが有効になっている場合、ユーザーはダイレクト メッセージとルームで共有されているファイルをダウンロードできます。ダウンロードが無効になっ ている場合、これらのファイルをプレビューしてファイルタブにアップロードすることしかできませ んが、ダウンロードすることはできません。ユーザーもスクリーンショットの撮影が制限されます。 試行すると黒い画面になります。

Note

ファイルのダウンロードが無効になっている場合、このファイル設定を適用するには、その セキュリティグループ内のすべてのユーザーが Wickr バージョン 6.54 以降を使用している 必要があります。

(フェデレーションによる)さまざまなネットワークとセキュリティグループのユーザーが いる部屋では、各ユーザーがファイルをプレビューまたはダウンロードできるかどうかは、 特定のセキュリティグループ設定に基づきます。その結果、一部のユーザーはルーム内の ファイルをダウンロードでき、他のユーザーはプレビューのみできます。

AWS Wickr でユーザーを管理する

Wickr AWS Management Console の のユーザー管理セクションでは、現在の Wickr ユーザーとボットを表示し、詳細を変更できます。

トピック

- AWS Wickr ネットワークのチームディレクトリ
- AWS Wickr ネットワークのゲストユーザー

AWS Wickr ネットワークのチームディレクトリ

現在の Wickr ユーザーを表示し、Wickr AWS Management Console の のユーザー管理セクションで 詳細を変更できます。

トピック

- AWS Wickr ネットワークでユーザーを表示する
- AWS Wickr ネットワークでユーザーを招待する
- AWS Wickr ネットワークでユーザーを編集する
- AWS Wickr ネットワークでユーザーを削除する
- AWS Wickr ネットワークのユーザーを一括削除する
- AWS Wickr ネットワークのユーザーを一括停止する

AWS Wickr ネットワークでユーザーを表示する

Wickr ネットワークに登録されているユーザーの詳細を表示できます。

Wickr ネットワークに登録されているユーザーを表示するには、次の手順を実行します。

- 1. 「https://<u>https://console.aws.amazon.com/wickr/</u>.com で Wickr AWS Management Console の を 開きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、ユーザー管理を選択します。

チームディレクトリタブには、名前、E メールアドレス、割り当てられたセキュリティグループ、現在のステータスなど、Wickr ネットワークに登録されているユーザーが表示されます。現

在のユーザーについては、デバイスの表示、詳細の編集、一時停止、削除、別の Wickr ネット ワークへの切り替えを行うことができます。

AWS Wickr ネットワークでユーザーを招待する

Wickr ネットワークでユーザーを招待できます。

Wickr ネットワークでユーザーを招待するには、次の手順を実行します。

- 1. 「https://<u>https://console.aws.amazon.com/wickr/</u>.com で Wickr AWS Management Console の を 開きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、ユーザー管理を選択します。
- 4. チームディレクトリタブで、ユーザーを招待を選択します。
- ユーザー招待ページで、ユーザーの E メールアドレスとセキュリティグループを入力します。E メールアドレスとセキュリティグループは、必須の唯一のフィールドです。ユーザーに適した セキュリティグループを必ず選択してください。Wickr は、ユーザーに指定したアドレスに招待 メールを送信します。
- 6. [Invite user] を選択します。

メールがユーザーに送信されます。このEメールには、Wickr クライアントアプリケーションの ダウンロードリンクと Wickr に登録するためのリンクが記載されています。ユーザーがEメー ル内のリンクを使用して Wickr に登録すると、Wickr チームディレクトリのステータスが 保留 中 から アクティブ に変わります。

AWS Wickr ネットワークでユーザーを編集する

Wickr ネットワークでユーザーを編集できます。

ユーザーを編集するには、次の手順を実行します。

- 1. Wickr AWS Management Console のを <u>https://console.aws.amazon.com/wickr/</u>://https//https
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、ユーザー管理を選択します。

- チームディレクトリタブで、編集するユーザーの縦の省略記号 (3 つのドット) アイコンを選択 します。
- 5. [編集]を選択します。
- 6. ユーザー情報を編集し、変更の保存を選択します。

AWS Wickr ネットワークでユーザーを削除する

Wickr ネットワーク内のユーザーを削除できます。

ユーザーを削除するには、次の手順を実行します。

- 1. Wickr AWS Management Console のを <u>https://console.aws.amazon.com/wickr/</u>://https//https//http
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、ユーザー管理を選択します。
- チームディレクトリタブで、削除するユーザーの縦の省略記号 (3 つのドット) アイコンを選択 します。
- 5. ユーザーを削除するには、[削除]を選択します。

ユーザーを削除すると、そのユーザーは Wickr クライアントで Wickr ネットワークにサインイ ンできなくなります。

6. ポップアップウィンドウで、[削除] を選択します。

AWS Wickr ネットワークのユーザーを一括削除する

Wickr ネットワークユーザーを一括削除するには、「 for Wickr AWS Management Console 」 の「ユーザー管理」セクションを参照してください。

Note

ユーザーを一括削除するオプションは、SSO が有効になっていない場合にのみ適用されま す。

CSV テンプレートを使用して Wickr ネットワークユーザーの一括を削除するには、次の手順を実行 します。

- 1. Wickr AWS Management Console の を「https://<u>https://console.aws.amazon.com/wickr/</u>.」で開 きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、ユーザー管理を選択します。
- 4. チームディレクトリタブには、Wickr ネットワークに登録されているユーザーが表示されます。
- 5. チームディレクトリタブで、ユーザーの管理を選択し、一括削除を選択します。
- ユーザーを一括削除するページで、サンプル CSV テンプレートをダウンロードします。サンプ ルテンプレートをダウンロードするには、テンプレートのダウンロードを選択します。
- 7. ネットワークから一括削除するユーザーの E メールを追加して、テンプレートを完了します。
- 完成した CSV テンプレートをアップロードします。ファイルをアップロードボックスにドラッ グアンドドロップするか、[ファイルを選択]を選択します。
- チェックボックスをオンにすると、ユーザーの削除は元に戻せないことがわかります。
- 10. ユーザーの削除を選択します。

この操作ではただちにユーザーの削除が開始され、数分かかる場合があります。削除したユーザーは、Wickr クライアントで Wickr ネットワークにサインインできなくなります。

チームディレクトリの CSV をダウンロードして Wickr ネットワークユーザーを一括削除するには、 次の手順を実行します。

- 1. 「https://<u>https://console.aws.amazon.com/wickr/</u>.com で Wickr AWS Management Console の を 開きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、ユーザー管理を選択します。
- 4. チームディレクトリタブには、Wickr ネットワークに登録されているユーザーが表示されます。
- 5. チームディレクトリタブで、ユーザーの管理を選択し、CSV としてダウンロードを選択します。
- チームディレクトリ CSV テンプレートをダウンロードしたら、削除する必要のないユーザーの 行を削除します。

- 7. チームディレクトリタブで、ユーザーの管理を選択し、一括削除を選択します。
- ユーザーー括削除ページで、チームディレクトリ CSV テンプレートをアップロードします。
 アップロードボックスにファイルをドラッグアンドドロップするか、ファイルの選択を選択します。
- 9. チェックボックスをオンにすると、ユーザーの削除は元に戻せないことがわかります。
- 10. ユーザーの削除を選択します。

この操作ではただちにユーザーの削除が開始され、数分かかる場合があります。削除し たユーザーは、Wickr クライアントで Wickr ネットワークにサインインできなくなりま す。

AWS Wickr ネットワークのユーザーを一括停止する

Wickr ネットワークユーザーを一括停止するには、「 for Wickr AWS Management Console 」 の「ユーザー管理」セクションを参照してください。

Note

ユーザーを一括停止するオプションは、SSO が有効になっていない場合にのみ適用されます。

Wickr ネットワークユーザーの一括利用を停止するには、次の手順を実行します。

- 1. 「https://<u>https://console.aws.amazon.com/wickr/</u>.com で Wickr AWS Management Console の を 開きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、ユーザー管理を選択します。
- 4. チームディレクトリタブには、Wickr ネットワークに登録されているユーザーが表示されます。
- 5. チームディレクトリタブで、ユーザーの管理を選択し、一括停止を選択します。
- ユーザーを一括停止ページで、サンプル CSV テンプレートをダウンロードします。サンプルテンプレートをダウンロードするには、テンプレートのダウンロードを選択します。

- ネットワークから一括停止したいユーザーのメールアドレスを追加して、テンプレートを完成させます。
- 完成した CSV テンプレートをアップロードします。ファイルをアップロードボックスにドラッ グアンドドロップするか、[ファイルを選択]を選択します。
- 9. ユーザーを停止を選択します。

この操作を行うと、ただちにユーザーの利用停止が開始され、数分かかる場合がありま す。利用停止中のユーザーは、Wickr クライアントで Wickr ネットワークにサインイン できません。現在クライアントで Wickr ネットワークにサインインしているユーザーを 一時停止すると、そのユーザーは自動的にサインアウトされます。

AWS Wickr ネットワークのゲストユーザー

Wickr ゲストユーザー機能を使用すると、個々のゲストユーザーが Wickr クライアントにサインイン し、Wickr ネットワークユーザーと共同作業を行うことができます。Wickr 管理者は、Wickr ネット ワークのゲストユーザーを有効または無効にできます。

この機能を有効にすると、Wickr ネットワークに招待されたゲストユーザーは、Wickr ネットワーク 内のユーザーとやり取りできるようになります。 AWS アカウント ゲストユーザー機能の には料金 が適用されます。ゲストユーザー機能の料金について詳しくは、「アドオンの料金設定」の「<u>Wickr</u> 料金ページ」を参照してください。

トピック

- AWS Wickr ネットワークでゲストユーザーを有効または無効にする
- AWS Wickr ネットワークでゲストユーザー数を表示する
- AWS Wickr ネットワークでの毎月の使用状況を表示する
- AWS Wickr ネットワークでゲストユーザーを表示する
- AWS Wickr ネットワークでゲストユーザーをブロックする

AWS Wickr ネットワークでゲストユーザーを有効または無効にする

Wickr ネットワークでゲストユーザーを有効または無効にできます。

Wickr ネットワークのゲストユーザーを有効または無効にするには、以下の手順を実行します。

- 1. 「https://<u>https://console.aws.amazon.com/wickr/</u>.com で Wickr AWS Management Console の を 開きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、[Security Groups] (セキュリティグループ) を選択します。
- 4. 特定のセキュリティグループの名前を選択します。

Note

ゲストユーザーは個々のセキュリティグループでのみ有効にできます。Wickr ネット ワーク内のすべてのセキュリティグループでゲストユーザーを有効にするには、ネット ワーク内のセキュリティグループごとにこの機能を有効にする必要があります。

- 5. セキュリティグループのフェデレーションタブを選択します。
- 6. ゲストユーザーを有効にするオプションが使用できる場所は 2 つあります。
 - ローカルフェデレーション 米国東部 (バージニア北部)のネットワークの場合は、ページのローカルフェデレーションセクションで編集を選択します。
 - グローバルフェデレーション 他のリージョンの他のすべてのネットワークについては、
 ページのグローバルフェデレーションセクションで編集を選択します。
- 7. フェデレーションの編集ページで、フェデレーションを有効にするを選択します。
- 8. 変更を保存を選択して変更を保存し、セキュリティグループに対して有効にします。

これで、Wickr ネットワーク内の特定のセキュリティグループの登録ユーザーがゲストユーザー とやり取りできるようになります。詳細については、「Wickr ユーザーガイド」の「<u>ゲストユー</u> ザー」を参照してください。

AWS Wickr ネットワークでゲストユーザー数を表示する

Wickr ネットワークでゲストユーザー数を表示できます。

Wickr ネットワークのゲストユーザー数を表示するには、以下の手順を実行します。

- 1. Wickr AWS Management Console の を <u>https://console.aws.amazon.com/wickr/</u>://www..com で開 きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。

3. ナビゲーションペインで、ユーザー管理を選択します。

ユーザー管理ページには、Wickr ネットワーク内のゲストユーザーの数が表示されます。

AWS Wickr ネットワークでの毎月の使用状況を表示する

請求期間中にネットワークが通信したゲストユーザーの数を表示できます。

Wickr ネットワークの毎月の使用状況を表示するには、次の手順を実行します。

- 1. Wickr AWS Management Console の を <u>https://console.aws.amazon.com/wickr/</u>://www..com で開 きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、ユーザー管理を選択します。
- 4. ゲストユーザータブを選択します。

ゲストユーザータブには、ゲストユーザーの毎月の使用状況が表示されます。

Note

ゲストの請求データは 24 時間ごとに更新されます。

AWS Wickr ネットワークでゲストユーザーを表示する

特定の請求期間中にネットワークユーザーが通信したゲストユーザーを表示できます。

特定の請求期間中にネットワークユーザーが通信したゲストユーザーを表示するには、次の手順を実 行します。

- 1. 「https://<u>https://console.aws.amazon.com/wickr/</u>.com で Wickr AWS Management Console の を 開きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、ユーザー管理を選択します。
- 4. ゲストユーザータブを選択します。

ゲストユーザータブには、ネットワーク内のゲストユーザーが表示されます。

毎月の使用状況の表示

AWS Wickr ネットワークでゲストユーザーをブロックする

Wickr ネットワークでゲストユーザーをブロックおよびブロック解除できます。ブロックされたユー ザーは、ネットワーク内の誰とも通信できません。

ゲストユーザーをブロックするには

- 1. Wickr AWS Management Console の を <u>https://console.aws.amazon.com/wickr/</u>://www..com で開 きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、ユーザー管理を選択します。
- 4. ゲストユーザータブを選択します。

ゲストユーザータブには、ネットワーク内のゲストユーザーが表示されます。

- 5. [ゲストユーザー] セクションで、ブロックしたいゲストユーザーの E メールを探します。
- 6. ゲストユーザー名の右側で、3つのドットを選択し、ゲストユーザーをブロックを選択します。
- 7. ポップアップウィンドウで [ブロック] を選択します。
- Wickr ネットワークでブロックされたユーザーのリストを表示するには、ステータスドロップダウンメニューを選択し、ブロックを選択します。

ゲストユーザーのブロックを解除するには

- 1. Wickr AWS Management Console のを <u>https://console.aws.amazon.com/wickr/</u>://https//https
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、ユーザー管理を選択します。
- 4. ゲストユーザータブを選択します。

ゲストユーザータブには、ネットワーク内のゲストユーザーが表示されます。

- 5. Status ドロップダウンメニューを選択し、Blocked を選択します。
- 6. ブロック セクションで、ブロックを解除するゲストユーザーの E メールを見つけます。
- 7. ゲストユーザー名の右側で、3つのドットを選択し、ユーザーのブロック解除を選択します。
- 8. ポップアップウィンドウでブロック解除を選択します。

AWS Wickr のセキュリティ

でのクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する 組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを活用できま す。

セキュリティは、 AWS お客様とお客様の間の責任共有です。<u>責任共有モデル</u>では、これをクラウ ドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ AWS は、で AWS サービスを実行するインフラストラクチャを保護す る責任を担います AWS クラウド。 AWS また、は、お客様が安全に使用できるサービスも提供し ます。サードパーティーの監査者は、<u>AWS コンプライアンスプログラム</u>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 Wickr に適 用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラム<u>AWS に</u> 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、 ユーザーは、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても 責任を負います。

このドキュメントは、Wickr を使用する際に責任共有モデルを適用する方法を理解するのに役立ちま す。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために Wickr を 設定する方法を示します。また、Wickr リソースのモニタリングや保護に役立つ他の AWS サービス の使用方法についても説明します。

トピック

- AWS Wickr でのデータ保護
- AWS Wickr の ID とアクセス管理
- コンプライアンス検証
- AWS Wickr の耐障害性
- AWS Wickr のインフラストラクチャセキュリティ
- AWS Wickr での設定と脆弱性の分析
- AWS Wickr のセキュリティのベストプラクティス

AWS Wickr でのデータ保護

責任 AWS <u>共有モデル</u>、AWS Wickr でのデータ保護に適用されます。このモデルで説明されている ように、AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を 維持する責任があります。また、使用する「AWS のサービス」のセキュリティ設定と管理タスク もユーザーの責任となります。データプライバシーの詳細については、<u>データプライバシーに関する</u> <u>よくある質問</u>を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブロ グに投稿された AWS 責任共有モデルおよび GDPR のブログ記事を参照してください。

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

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

お客様のEメールアドレスなどの極秘または機密情報を、タグ、または[名前] フィールドなどの自 由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、また は SDK を使用して Wickr AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求また は診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへの リクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

AWS Wickr の ID とアクセス管理

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、Wickr リソースを使用するための 認証 (サインイン) および 許可 (アクセス許可を持たせる) を行うことができる人を制御します。IAM は、 追加料金なしで使用できる AWS のサービス です。

トピック

- ・ <u>AWS Wickr の対象者</u>
- AWS Wickr の ID を使用した認証
- AWS Wickr のポリシーを使用したアクセスの管理
- AWS AWS Wickr の マネージドポリシー
- ・ AWS Wickr と IAM の連携方法
- AWS Wickr のアイデンティティベースのポリシーの例
- AWS Wickr の ID とアクセスのトラブルシューティング

AWS Wickr の対象者

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

サービスユーザー – Wickr サービスを使用してジョブを実行する場合は、必要な認証情報とアクセス 許可を管理者が提供します。作業を実行するためにさらに多くの Wickr の機能を使用するとき、追 加の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すると、管理者に適切なアクセ ス許可をリクエストするのに役に立ちます。Wickr の特徴にアクセスできない場合は、「<u>AWS Wickr</u> の ID とアクセスのトラブルシューティング」を参照してください。

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

IAM 管理者 - 管理者は、Wickr へのアクセスを管理するポリシーの作成方法の詳細について確認す る場合があります。IAM で使用できる Wickr 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、AWS Wickr のアイデンティティベースのポリシーの例 を参照してください。

AWS Wickr の ID を使用した認証

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

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインイ ンできます。 AWS IAM Identity Center (IAM Identity Center) ユーザー、会社のシングルサインオン 認証、Google または Facebook 認証情報は、フェデレーション ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーション が設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引 き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインイ ンできます。へのサインインの詳細については AWS、「 AWS サインイン ユーザーガイド<u>」の「 へ</u> のサインイン AWS アカウント方法」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を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。リクエストに自分 で署名する推奨方法の使用については、「IAM ユーザーガイド」の「<u>API リクエストに対するAWS</u> Signature Version 4」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。たと えば、 では、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「<u>多要素認証</u>」お よび「IAM ユーザーガイド」の「IAM のAWS 多要素認証」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウ ント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサイ ンインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強く お勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実 行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストに ついては、「IAM ユーザーガイド」の「<u>ルートユーザー認証情報が必要なタスク</u>」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、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 AWS のサービス を使用して に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 ンを使用することを要求します。

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 にアクセスするユーザーです。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、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するか、独自の ID ソースのユーザーとグループのセッ トに接続して同期し、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「<u>What is IAM Identity</u> <u>Center</u>?」(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 ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内の 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保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

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

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

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内の ID です。これは IAM ユーザーに 似ていますが、特定のユーザーには関連付けられていません。で IAM ロールを一時的に引き受ける には AWS Management Console、ユーザーから IAM ロール (コンソール) に切り替える ことができ ます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタ ム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「ロー ルを引き受けるための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス フェデレーティッド ID に許可を割り当てるには、ロール を作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID は ロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロール については、「IAM ユーザーガイド」の「<u>サードパーティー ID プロバイダー (フェデレーション)</u> <u>用のロールを作成する</u>」を参照してください。IAM Identity Center を使用する場合は、許可セッ トを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、 「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。
- 一時的な IAM ユーザー権限 IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる 権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、(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におけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。
- クロスサービスアクセス 一部の は他の の機能 AWS のサービス を使用します AWS のサービ ス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプ リケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスで は、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこ れを行う場合があります。
 - 転送アクセスセッション (FAS) IAM ユーザーまたはロールを使用して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 へのリクエストをリクエストする と組み合わせて使用します。FAS リクエストは、サービス が他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け 取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必 要です。FAS リクエストを行う際のポリシーの詳細については、「<u>転送アクセスセッション</u>」 を参照してください。

- サービスロール サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができま す。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを 作成する」を参照してください。
- サービスにリンクされたロール サービスにリンクされたロールは、にリンクされたサービス ロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行する ロールを引き受けることができます。サービスにリンクされたロールはに表示され AWS アカ ウント、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許 可を表示できますが、編集することはできません。
- Amazon EC2 で実行されているアプリケーション IAM ロールを使用して、EC2 インスタンスで 実行され、AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を 管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 イン スタンスに AWS ロールを割り当て、そのすべてのアプリケーションで使用できるようにするに は、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロ ファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を 取得できます。詳細については、「IAM ユーザーガイド」の「<u>Amazon EC2 インスタンスで実行</u> されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

AWS Wickr のポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。 ポリシーは 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 のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッ ション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限によ り、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメ ント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、 「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、ど のプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということで す。 デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアク ションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者 はロールに IAM ポリシーを追加し、ユーザーはロールを引き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方法を問わず、アクションの許可を定義します。例え ば、iam:GetRole アクションを許可するポリシーがあるとします。そのポリシーを持つユーザー は、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、 アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、 ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデン ティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「<u>カスタマー管理ポリ</u> シーでカスタム IAM アクセス許可を定義する」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類 できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれてい ます。管理ポリシーは、内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロン ポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシー が含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法について は、「IAM ユーザーガイド」の「<u>管理ポリシーとインラインポリシーのいずれかを選択する</u>」を参 照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソース ベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげ られます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを 使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの 場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーに よって定義されます。リソースベースのポリシーでは、<u>プリンシパルを指定する</u>必要があります。プ リンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含める ことができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポ リシーでは、IAM の AWS マネージドポリシーを使用できません。 アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、または ロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリ シーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、および Amazon VPC は AWS WAF、ACLs。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「<u>アクセスコントロールリスト (ACL) の概要</u>」を参 照してください。

その他のポリシータイプ

AWS は、一般的でない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティに許可の境界を設定できます。結果として許可される範囲は、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、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。
- セッションポリシー セッションポリシーは、ロールまたはフェデレーションユーザーの一時的な セッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果として セッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポ リシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もありま す。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細について は、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解する のがさらに難しくなります。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<u>「ポリシー評価ロジック</u>」を参照し てください。

AWS AWS Wickr の マネージドポリシー

ユーザー、グループ、ロールにアクセス許可を追加するには、自分でポリシーを記述するよりも AWS 管理ポリシーを使用する方が簡単です。チームに必要な権限のみを提供する <u>IAM カスタマーマ</u> <u>ネージドポリシーを作成する</u>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、IAM ユーザーガイ ドの「 AWS 管理ポリシー」を参照してください。

AWS のサービス AWS 管理ポリシーを維持および更新します。 AWS 管理ポリシーのアクセス許可 は変更できません。サービスでは新しい機能を利用できるようにするために、 AWS マネージドポリ シーに権限が追加されることがあります。この種類の更新はポリシーがアタッチされている、すべて のアイデンティティ (ユーザー、グループおよびロール) に影響を与えます。新しい機能が立ち上げ られた場合や、新しいオペレーションが使用可能になった場合に、各サービスが AWS マネージドポ リシーを更新する可能性が最も高くなります。サービスは AWS マネージドポリシーからアクセス許 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。

AWS マネージドポリシー: AWSWickrFullAccess

AWSWickrFullAccess ポリシーを IAM アイデンティティにアタッチできます。このポリシーは、 AWS Management Console内の Wickr の AWS Management Console を含む、Wickr サービスに対 する完全な管理権限を付与します。IAM アイデンティティへのポリシーのアタッチに関する詳細に ついては、「AWS Identity and Access Management IAM ユーザーガイド」の「<u>IAM ID の許可の追加</u> と削除」を参照してください。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

• wickr—Wickrサービスに完全な管理者権限を付与します。

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

}

AWS 管理ポリシーの Wickr 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 Wickr 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。このページへの変更に関する自動アラートを受信するには、Wickr ドキュメ ント履歴ページで RSS フィードを購読してください。

変更	説明	日付
<u>AWSWickrFullAccess</u> — 新し いポリシー	Wickr は、AWS Managemen t Consoleの Wickr 管理者コン ソールを含む Wickr サービス に完全な管理者権限を付与す る新しいポリシーを追加しま した。	2022 年 11 月 28 日
Wickr は変更の追跡を開始し ました	Wickr は、 AWS 管理ポリシー の変更の追跡を開始しまし た。	2022 年 11 月 28 日

AWS Wickr と IAM の連携方法

IAM を使用して Wickr へのアクセスを管理する前に、Wickr で利用できる IAM の機能について学びます。

AWS Wickr で使用できる IAM 機能

IAM 機能	Wickr サポート
<u>アイデンティティベースポリシー</u>	はい
<u>リソースベースのポリシー</u>	いいえ
<u>ポリシーアクション</u>	はい
ポリシーリソース	いいえ

IAM 機能	Wickr サポート
<u>ポリシー条件キー</u>	いいえ
ACL	いいえ
<u>ABAC (ポリシー内のタグ)</u>	いいえ
一時的な認証情報	いいえ
<u>プリンシパル権限</u>	いいえ
サービスロール	いいえ
サービスリンクロール	いいえ

Wickr およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要について は、IAM ユーザーガイドの<u>AWS 「IAM と連携する のサービス</u>」を参照してください。

Wickr のアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、 アイデンティティにアタッチできる JSON 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 スのポリシーの作成方法については、「IAM ユーザーガイド」の「<u>カスタマー管理ポリシーでカス</u> タム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およ びアクションを許可または拒否する条件を指定できます。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学ぶには、「IAM ユーザーガイド」の「<u>IAM</u> JSON ポリシーの要素のリファレンス」を参照してください。

Wickr のアイデンティティベースのポリシーの例

Wickr のアイデンティティベースのポリシーの例を表示するには、「<u>AWS Wickr のアイデンティ</u> ティベースのポリシーの例」を参照してください。 Wickr 内のリソースベースのポリシー

リソースベースのポリシーのサポート:なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソース ベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげ られます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを 使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの 場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーに よって定義されます。リソースベースのポリシーでは、<u>プリンシパルを指定する</u>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、アカウント全体、または別のアカウントの IAM エン ティティをリソースベースのポリシーのプリンシパルとして指定します。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「IAM でのクロスアカウントリソー スアクセス」を参照してください。

Wickr のポリシーアクション

ポリシーアクションのサポート:あり

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

JSON ポリシーの Action 要素にはポリシー内のアクセスを許可または拒否するために使用できる アクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレー ションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例 外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追 加アクションは依存アクションと呼ばれます。

このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシー で使用されます。 Wickr アクションのリストを確認するには、サービス認可リファレンス の「<u>AWS Wickr で定義され</u> るアクション」を参照してください。

Wickr のポリシーアクションは、アクションの前に以下のプレフィックス を使用します。

wickr

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": [
    "wickr:action1",
    "wickr:action2"
]
```

Wickr のアイデンティティベースのポリシーの例を表示するには、「<u>AWS Wickr のアイデンティ</u> ティベースのポリシーの例」を参照してください。

Wickr のポリシーリソース

ポリシーリソースのサポート:なし

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

Resource JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。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、<u>Amazon リソースネーム (ARN)</u>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": "*"

Wickr リソースタイプとその ARN のリストを表示するには、サービス認可リファレンス の「<u>AWS</u> <u>Wickr によって定義されたリソース</u>」を参照してください。どのアクションで各リソースの ARN を 指定できるかについては、AWS Wickr で定義されるアクションを参照してください。 Wickr のアイデンティティベースのポリシーの例を表示するには、「<u>AWS Wickr のアイデンティ</u> ティベースのポリシーの例」を参照してください。

Wickr 向けのポリシー条件キー

サービス固有のポリシー条件キーへのサポート:なし

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

Condition 要素 (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 <u>条件演算子</u> を使用して条件 式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。

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 ユーザーに、IAM ユーザー 名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細 については、「IAM ユーザーガイド」の「<u>IAM ポリシーの要素: 変数およびタグ</u>」を参照してくださ い。

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ています。すべての AWS グ ローバル条件キーを確認するには、「IAM ユーザーガイド」の<u>AWS 「グローバル条件コンテキスト</u> キー」を参照してください。

Wickr の条件キーのリストを確認するには、「サービス認可リファレンス」の「<u>AWS Wickr の条</u> <u>件キー</u>」を参照してください。どのアクションおよびリソースと条件キーを使用できるかについて は、AWS Wickr で定義されるアクションを参照してください。

Wickr のアイデンティティベースのポリシーの例を表示するには、「<u>AWS Wickr のアイデンティ</u> ティベースのポリシーの例」を参照してください。

Wickr の ACL

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、または ロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリ シーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Wickr での ABAC

ABAC (ポリシー内のタグ) のサポート: なし

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。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) およ び多くの 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、ABAC の最初 の手順です。その後、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した場 合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

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

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

ABAC の詳細については、「IAM ユーザーガイド」の「<u>ABAC 認可でアクセス許可を定義する</u>」を 参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM ユーザーガイド」の「<u>属性ベースのアクセスコントロール (ABAC) を使用する</u>」を参照してくださ い。

Wickr 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:なし

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 を使用する場合などの詳細については、IAM ユーザーガイドの「IAM AWS のサービス と連携する 」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は、一時 的な認証情報を使用します。たとえば、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。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「<u>ユー</u> ザーから IAM ロールに切り替える (コンソール)」を参照してください。

ー時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これら の一時的な認証情報を使用してアクセスすることができます 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、 「IAM の一時的セキュリティ認証情報」を参照してください。

Wickr のクロスサービスプリンシパル許可

転送アクセスセッション (FAS) のサポート: なし

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 へのリクエストをリクエストする と組み合 わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり 取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアク ションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細につ いては、「転送アクセスセッション」を参照してください。

Wickr のサービスロール

サービスロールのサポート:なし

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける <u>IAM</u> <u>ロール</u>です。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細につい ては、「IAM ユーザーガイド」の「<u>AWS のサービスに許可を委任するロールを作成する</u>」を参照し てください。

Marning

サービスロールの許可を変更すると、Wickr の機能が破損する可能性があります。 Wickr が 指示する場合以外は、サービスロールを編集しないでください。

Wickr のサービスリンクロール

サービスにリンクされたロールのサポート:なし

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

サービスにリンクされたロールの作成または管理の詳細については、「<u>IAM と提携するAWS のサー</u> <u>ビス</u>」を参照してください。表の「サービスリンクロール」列に Yes と記載されたサービスを見つ けます。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、Yes (は い) リンクを選択します。

AWS Wickr 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、まったく新しい IAM ユーザーには、何かを実行する許可は一切ありません。IAM 管 理者は、AWS Wickr サービスを管理するための許可をユーザーに付与する IAM ポリシーを作成して 割り当てる必要があります。以下に示しているのは、アクセス許可ポリシーの例です。

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

このサンプルポリシーは、Wickr AWS Management Console 用 を使用して Wickr ネットワークを作 成、表示、管理するアクセス許可をユーザーに付与します。IAM ポリシーステートメント内の要素 の詳細については、「<u>Wickr のアイデンティティベースのポリシー</u>」を参照してください。これらの JSON ポリシードキュメント例を使用して IAM 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「<u>JSON タブでのポリシーの作成</u>」を参照してください。

トピック

- ポリシーに関するベストプラクティス
- AWS Management Console を Wickr 用に使用する

• 自分の権限の表示をユーザーに許可する

ポリシーに関するベストプラクティス

アイデンティティベースのポリシーは、誰かがあなたのアカウントでWickrリソースを作成、アクセ ス、または削除できるかどうかを決定します。これらのアクションを実行すると、 AWS アカウント に料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする 際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する ユーザーとワークロードにア クセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めしま す。詳細については、「IAM ユーザーガイド」の「<u>AWS マネージドポリシー</u>」または「<u>ジョブ機</u> 能のAWS マネージドポリシー」を参照してください。
- 最小特権を適用する IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを 付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定 義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する 方法の詳細については、「IAM ユーザーガイド」の「<u>IAM でのポリシーとアクセス許可</u>」を参照 してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションがなどの特定のを通じて使用されている場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサ ポートします。詳細については、「IAM ユーザーガイド」の「<u>IAM Access Analyzer でポリシーを</u> 検証する」を参照してください。
- 多要素認証 (MFA) を要求する で IAM ユーザーまたはルートユーザーを必要とするシナリオがあ る場合は AWS アカウント、MFA をオンにしてセキュリティを強化します。API オペレーション が呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細につい ては、「IAM ユーザーガイド」の「MFA を使用した安全な API アクセス」を参照してください。

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

AWS Management Console を Wickr 用に使用する

AWSWickrFullAccess AWS 管理ポリシーを IAM ID にアタッチして、の Wickr 管理者コンソール を含む Wickr サービスへの完全な管理アクセス許可を付与します AWS Management Console。詳細 については、「AWS マネージドポリシー: AWSWickrFullAccess」を参照してください。

自分の権限の表示をユーザーに許可する

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

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

```
"iam:ListUsers"
],
"Resource": "*"
}
]
}
```

AWS Wickr の ID とアクセスのトラブルシューティング

次の情報は、Wickr と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立 ちます。

トピック

• Wickr AWS Management Console の で管理アクションを実行する権限がない

Wickr AWS Management Console ので管理アクションを実行する権限がない

AWS Management Console for Wickr でアクションを実行する権限がないと通知された場合は、管理 者に連絡してサポートを依頼する必要があります。管理者とは、サインイン認証情報を提供した担当 者です。

次の例のエラーは、IAM mateojackson ユーザーが AWS Management Console for Wickr を使用し て for Wickr で Wickr AWS Management Console ネットワークを作成、管理、または表示しようと しても、wickr:CreateAdminSessionおよび アクセスwickr:ListNetworks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: wickr:ListNetworks

この場合、Mateo は管理者にポリシーを更新して、 アクションwickr:CreateAdminSessionと wickr:ListNetworksアクションを使用して Wickr AWS Management Console の にアクセスする ことを許可するよう依頼します。詳細については、「<u>AWS Wickr のアイデンティティベースのポリ</u> シーの例」および「AWS マネージドポリシー: AWSWickrFullAccess」を参照してください。
コンプライアンス検証

特定のコンプライアンスプログラムの対象となる AWS サービスのリストについては、「コンプライ アンス<u>AWS プログラムによる対象範囲内のサービスコンプライアンス</u>」を参照してください。一般 的な情報については、AWS 「 Compliance ProgramsAssurance」を参照してください。

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

Wickr を使用する際のコンプライアンス責任は、データの機密性、貴社のコンプライアンス目標、適用される法律と規制によって決まります。 AWS は、コンプライアンスに役立つ次のリソースを提供します。

- 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 ベースライン環境をデプロイする手順について説明します AWS。
- <u>AWS コンプライアンスリソース</u> このワークブックとガイドのコレクションは、お客様の業界や 地域に適用される場合があります。
- 「デベロッパーガイド」の「ルールによるリソースの評価」 AWS Config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 Config
- <u>AWS Security Hub</u> この AWS サービスは、内のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスへの準拠を確認するのに役立ちます。

AWS Wickr の耐障害性

AWS グローバルインフラストラクチャは、AWS リージョン およびアベイラビリティーゾーンを中 心に構築されています。は、低レイテンシー、高スループット、高度に冗長なネットワークで接続 された、物理的に分離および分離された複数のアベイラビリティーゾーン AWS リージョン を提供 します。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーす るアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾー ンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォール トトレラントで、スケーラブルです。

AWS リージョン およびアベイラビリティーゾーンの詳細については、<u>AWS 「 グローバルインフラ</u> <u>ストラクチャ</u>」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、Wickr 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いくつかの機能を提供しています。詳細については、「<u>AWS Wickr の</u> データ保持」を参照してください。

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

AWS Wickr での設定と脆弱性の分析

設定と IT コントロールは、 AWS お客様と当社のお客様との間の責任共有です。詳細については、 AWS 「 責任共有モデル」を参照してください。

仕様とガイドラインに従って Wickr を設定し、定期的に最新バージョンの Wickr クライアントをダ ウンロードするようにユーザーに指示し、最新バージョンの Wickr データ保持ボットを実行してい ることを確認し、ユーザーによる Wickr の使用状況を監視するのはお客様の責任です。

AWS Wickr のセキュリティのベストプラクティス

Wickr 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る必要のあるいくつかの セキュリティ機能が用意されています。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 お客様の環境に適切ではないか、十分ではない場合があるため、これらは指示ではなく、有用な考慮 事項と見なしてください。

Wickr の使用に関連する潜在的なセキュリティイベントを防ぐには、以下のベストプラクティスに 従ってください。

- ・最小限の権限アクセスを実装し、Wickr アクションに使用する特定のロールを作成してください。IAM テンプレートを使用してロールを作成します。詳細については、「<u>AWS AWS Wickr の</u>マネージドポリシー」を参照してください。
- AWS Management Console を最初に認証して、AWS Management Console for Wickr にアクセス します。個人コンソールの認証情報は共有しないでください。インターネット上の誰でもコンソー ルにアクセスできますが、コンソールへの有効な認証情報がない限り、サインインしたりセッショ ンを開始したりすることはできません。

AWS Wickr のモニタリング

モニタリングは、AWS Wickr およびその他の AWS ソリューションの信頼性、可用性、パフォー マンスを維持する上で重要な部分です。 は、Wickr 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に以下のモニタリングツール AWS を提供します。

 AWS CloudTrail は、AWS アカウントによって、またはアカウントに代わって行われた API コー ルおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信しま す。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出 しの発生日時を特定できます。詳細については、AWS CloudTrail ユーザーガイドをご参照くださ い。CloudTrail を使用した Wickr API 呼び出しのログ記録の詳細については、「<u>を使用した AWS</u> Wickr API コールのログ記録 AWS CloudTrail」を参照してください。

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

AWS Wickr は、Wickr のユーザー AWS CloudTrail、ロール、または サービスによって実行され たアクションを記録する AWS サービスである と統合されています。CloudTrailはWickrのすべて のAPI コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、Wickr AWS Management Console の からの呼び出しと、Wickr API オペレーションへのコード呼び出しが含まれ ます。トレイルを作成すると、CloudTrailイベントをAmazon S3バケットに継続的に配信できるよう になります。追跡を設定しない場合でも、CloudTrail コンソールの Event history (イベント履歴) で 最新のイベントを表示できます。CloudTrailによって収集された情報を使用することで、Wickrに対 して行われたリクエスト、リクエストが行われたIPアドレス、リクエストを行った人、リクエスト が行われた日時、その他の詳細を特定することができます。CloudTrail の詳細については、「<u>AWS</u> <u>CloudTrail ユーザーガイド</u>」を参照してください。

CloudTrailのWickr情報

アカウントを作成する AWS アカウント と、 で CloudTrail が有効になります。Wickr でアクティ ビティが発生すると、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。最近のイベントは、 AWS アカウントで表示、検索、ダウン ロードできます。詳細については、 <u>CloudTrail イベント履歴でのイベントの表示</u>を参照してくださ い。

Wickr のイベントなど AWS アカウント、 のイベントの継続的な記録については、証跡を作成し ます。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォル トでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。 証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集したイベント データをより詳細に分析し、それに基づいて対応するため、他の AWS サービスを構成できます。詳 細については、次を参照してください:

- 追跡を作成するための概要
- 「CloudTrail がサポートされているサービスと統合」
- 「CloudTrail の Amazon SNS 通知の設定」
- ・「<u>複数のリージョンから CloudTrail ログファイルを受け取る</u>」および「<u>複数のアカウントから</u> <u>CloudTrail ログファイルを受け取る</u>」

WickrのすべてのアクションはCloudTrailによって記録されます。例えば、CreateAdminSession と ListNetworks の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されま す。

各イベントまたはログエントリには、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。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用 して行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用 して行われたかどうか。
- ・ リクエストが別の AWS サービスによって行われたかどうか。

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

Wickrのログファイルエントリーを理解します。

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設 定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意 ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエスト パラメータなどの情報を含みます。CloudTrail ログファイルは、パブリック API コールの順序付けら れたスタックトレースではないため、特定の順序では表示されません。

以下の例は、CreateAdminSession アクションを示す CloudTrail ログエントリです。

```
"eventVersion": "1.08",
   "userIdentity": {
       "type": "AssumedRole",
       "principalId": "<principal-id>",
       "arn": "<arn>",
       "accountId": "<account-id>",
       "accessKeyId": "<access-key-id>",
       "sessionContext": {
           "sessionIssuer": {
               "type": "Role",
               "principalId": "<principal-id>",
               "arn": "<arn>",
               "accountId": "<account-id>",
               "userName": "<user-name>"
           },
           "webIdFederationData": {},
           "attributes": {
               "creationDate": "2023-03-10T07:53:17Z",
               "mfaAuthenticated": "false"
           }
       }
   },
   "eventTime": "2023-03-10T08:19:24Z",
   "eventSource": "wickr.amazonaws.com",
   "eventName": "CreateAdminSession",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "<ip-address>",
   "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/110.0.0.0 Safari/537.36",
   "requestParameters": {
       "networkId": 56019692
   },
   "responseElements": {
       "sessionCookie": "***",
       "sessionNonce": "***"
   },
   "requestID": "39ed0e6f-36e9-460d-8a6e-f24be0ec11c5",
   "eventID": "98ccb633-0e6c-4325-8996-35c3043022ac",
   "readOnly": false,
   "eventType": "AwsApiCall",
   "managementEvent": true,
   "recipientAccountId": "<account-id>",
   "eventCategory": "Management"
```

}

{

以下の例は、CreateNetwork アクションを示す CloudTrail ログエントリです。

```
"eventVersion": "1.08",
   "userIdentity": {
       "type": "AssumedRole",
       "principalId": "<principal-id>",
       "arn": "<arn>",
       "accountId": "<account-id>",
       "accessKeyId": "<access-key-id>",
       "sessionContext": {
           "sessionIssuer": {
               "type": "Role",
               "principalId": "<principal-id>",
               "arn": "<arn>",
               "accountId": "<account-id>",
               "userName": "<user-name>"
           },
           "webIdFederationData": {},
           "attributes": {
               "creationDate": "2023-03-10T07:53:17Z",
               "mfaAuthenticated": "false"
           }
       }
   },
   "eventTime": "2023-03-10T07:54:09Z",
   "eventSource": "wickr.amazonaws.com",
   "eventName": "CreateNetwork",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "<ip-address>",
   "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/110.0.0.0 Safari/537.36",
   "requestParameters": {
       "networkName": "BOT_Network",
       "accessLevel": "3000"
   },
   "responseElements": null,
   "requestID": "b83c0b6e-73ae-45b6-8c85-9910f64d33a1",
   "eventID": "551277bb-87e0-4e66-b2a0-3cc1eff303f3",
   "readOnly": false,
   "eventType": "AwsApiCall",
```

```
"managementEvent": true,
"recipientAccountId": "<account-id>",
"eventCategory": "Management"
}
```

以下の例は、ListNetworks アクションを示す CloudTrail ログエントリです。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T12:19:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T12:29:32Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "ListNetworks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "b9800ba8-541a-43d1-9c8e-efd94d5f2115",
    "eventID": "5fbc83d7-771b-457d-9329-f85163a6a428",
    "readOnly": true,
    "eventType": "AwsApiCall",
```

```
"managementEvent": true,
"recipientAccountId": "<account-id>",
"eventCategory": "Management"
}
```

以下の例は、UpdateNetworkdetails アクションを示す CloudTrail ログエントリです。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T22:42:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T22:42:58Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "UpdateNetworkDetails",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkName": "CloudTrailTest1",
        "networkId": <network-id>
    },
    "responseElements": null,
    "requestID": "abced980-23c7-4de1-b3e3-56aaf0e1fdbb",
```

```
"eventID": "a4dc3391-bdce-487d-b9b0-6f76cedbb198",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "<account-id>",
"eventCategory": "Management"
}
```

以下の例は、TagResource アクションを示す CloudTrail ログエントリです。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T22:42:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T23:06:04Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "resource-arn": "<arn>",
        "tags": {
```

```
"some-existing-key-3": "value 1"
}
},
"responseElements": null,
"requestID": "4ff210e1-f69c-4058-8ac3-633fed546983",
"eventID": "26147035-8130-4841-b908-4537845fac6a",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "<account-id>",
"eventCategory": "Management"
}
```

以下の例は、ListTagsForResource アクションを示す CloudTrail ログエントリです。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<access-key-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T18:50:37Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T18:50:37Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "ListTagsForResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
```

```
"userAgent": "axios/0.27.2",
    "errorCode": "AccessDenied",
    "requestParameters": {
        "resource-arn": "<arn>"
    },
    "responseElements": {
        "message": "User: <arn> is not authorized to perform: wickr:ListTagsForResource
 on resource: <arn> with an explicit deny"
    },
    "requestID": "c7488490-a987-4ca2-a686-b29d06db89ed",
    "eventID": "5699d5de-3c69-4fe8-b353-8ae62f249187",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

AWS Wickr の分析ダッシュボード

分析ダッシュボードを使用して、組織が AWS Wickr をどのように活用しているかを確認できます。 次の手順では、AWS Wickr コンソールを使用して分析ダッシュボードにアクセスする方法について 説明します。

分析ダッシュボードにアクセスするには

- 1. 「https://<u>https://console.aws.amazon.com/wickr/</u>.com で Wickr AWS Management Console の を 開きます。
- 2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
- 3. ナビゲーションペインで、[Analytics] を選択します。

Analytics ページには、ネットワークのメトリクスがさまざまなタブに表示されます。

分析ページには、各タブの右上隅に時間枠フィルターがあります。このフィルターはページ全体に適 用されます。さらに、各タブの右上隅で、使用可能なエクスポートオプションを選択して、選択した 時間範囲のデータポイントをエクスポートできます。

Note

選択した時刻は UTC (協定世界時) です。

次のタブを使用できます。

- 概要は以下を表示します。
 - ・登録済み 選択した時間内のネットワーク上のアクティブユーザーと停止ユーザーを含む、登録済みユーザーの総数。保留中または招待されたユーザーは含まれません。
 - 保留中 選択した時間内のネットワーク上の保留中のユーザーの総数。
 - ユーザー登録 グラフには、選択した時間範囲に登録されたユーザーの総数が表示されます。
 - デバイス アプリがアクティブになっているデバイスの数。
 - クライアントバージョン クライアントバージョンによって分類されたアクティブなデバイスの数。
- メンバーには以下が表示されます。
 - ステータス 選択した期間内にネットワーク上のアクティブなユーザー。
 - アクティブなユーザー
 - グラフには、アクティブユーザーの数を経時的に表示し、日単位、週単位、または月単位(上記で選択した時間範囲内)で集計できます。
 - アクティブなユーザー数は、プラットフォーム、クライアントバージョン、またはセキュ リティグループ別に分類できます。セキュリティグループが削除された場合、合計数は Deleted#と表示されます。
- メッセージは以下を表示します。
 - ・送信されたメッセージ 選択した期間にネットワーク上のすべてのユーザーとボットによって
 送信された一意のメッセージの数。
 - 呼び出し ネットワーク内のすべてのユーザーが行った一意の呼び出しの数。
 - ファイル ネットワーク内のユーザーが送信したファイルの数(音声メモを含む)。
 - デバイス 円グラフには、オペレーティングシステム別に分類されたアクティブなデバイスの 数が表示されます。

クライアントバージョン — クライアントバージョンによって分類されたアクティブなデバイスの数。

ドキュメント履歴

以下の表は、Wickrのドキュメントのリリースについて説明したものです。

変更	説明	日付
<u>ファイルプレビューが利用可</u> <u>能になりました</u>	Wickr 管理者は、ファイルの ダウンロードを有効または無 効にできるようになりました 。詳細については、 <u>「AWS</u> <u>Wickr のファイルプレビュ</u> <u>ー</u> 」を参照してください。	2025 年 5 月 29 日
<u>新しく再設計された Wickr 管</u> 理者コンソールが利用可能に なりました	Wickr は、Wickr 管理者コン ソールを拡張して、管理者の ナビゲーションとアクセシビ リティを向上させました。	2025 年 3 月 13 日
<u>Wickr がアジアパシフィック</u> (マレーシア) で利用可能にな りました AWS リージョン	Wickr がアジアパシフィック (マレーシア) で利用可能にな りました AWS リージョン。 詳細については、 <u>「リージョ</u> <u>ンの可用性</u> 」を参照してくだ さい。	2024 年 11 月 20 日
<u>削除ネットワークが利用可能</u> <u>になりました</u>	Wickr 管理者は、AWS Wickr ネットワークを削除できるよ うになりました。詳細につい ては、 <u>「AWS Wickr でネット</u> <u>ワークを削除する</u> 」を参照し てください。	2024 年 10 月 4 日
<u>Microsoft Entra (Azure AD)</u> <u>SSO を使用した AWS Wickr</u> の設定が利用可能になりまし <u>た</u>	AWS Wickr は、Microsoft Entra (Azure AD) を ID プロバ イダーとして使用するように 設定できます。詳細について は、「Configure AWS Wickr	2024 年 9 月 18 日

with Microsoft Entra (Azure AD) single sign-on」を参照し てください。

Wickr が欧州 (チューリッヒ) で利用可能に AWS リージョ ン

クロス境界分類とフェデレー ションが利用可能になりまし た

読み取り受信機能が使用可能 になりました

Wickr が欧州 (チューリッヒ) 2024 年 8 月 12 日 で利用可能になりました AWS リージョン。詳細について は、「リージョンの可用性」 を参照してください。

クロス境界分類機能を使用 すると、GovCloud ユーザー の会話に対するユーザーイ ンターフェイスの変更が可 能になります。詳細について は、GovCloud クロス境界分類 とフェデレーション」を参照 してください。

Wickr 管理者は、管理者コン ソールで読み取り受信機能を 有効または無効にできるよう になりました。詳細について は、「受信の読み取り」を参 照してください。

2024 年 6 月 25 日

2024 年 4 月 23 日

<u>グローバルフェデレーション</u> <u>で制限付きフェデレーション</u> <u>がサポートされ、管理者は管</u> 理者コンソールで使用状況分 <u>析を表示できるようになりま</u> した。

<u>AWS Wickr の Premium プラ</u> ンの 3 か月間の無料トライア ルが利用可能に グローバルフェデレーション が制限付きフェデレーショ ンをサポートするようになり ました。これは、他の Wickr ネットワークで機能します AWS リージョン。詳しくは<u>セ</u> <u>キュリティグループ</u>を参照 してください。さらに、管 理者は 管理者コンソールの Analytics ダッシュボードで使 用状況分析を表示できるよう になりました。詳細について は、「分析ダッシュボード」 を参照してください。

Wickr 管理者は、最大 30 人の ユーザーに対して 3 か月間の 無料トライアル Premium プラ ンを選択できるようになりま した。無料トライアル中は、 無制限の管理コントロールや データ保持など、スタンダー ドプランとプレミアムプラン のすべての機能を利用できま す。ゲストユーザー機能は、 プレミアム無料トライアル中 は利用できません。詳細につ いては、「プランの管理」を 参照してください。

2024年3月28日

2024年2月9日

<u>ゲストユーザー機能が一般公</u> <u>開され、より多くの管理者コ</u> <u>ントロールが追加されまし</u> <u>た。</u>	Wickr 管理者は、ゲストユー ザーのリスト、ユーザーのー 括削除または利用停止、ゲス トユーザーの Wickr ネット ワーク内での通信をブロック するオプションなど、さまざ まな新機能にアクセスできる ようになりました。詳細につ いては、「 <u>ゲストユーザー</u> 」 を参照してください。	2023 年 11 月 8 日
<u>Wickr が欧州 (フランクフルト)</u> <u>で利用可能に AWS リージョ</u> <u>ン</u>	Wickr が欧州 (フランクフル ト) で利用可能になりました AWS リージョン。詳細につ いては、 <u>「リージョンの可用</u> <u>性</u> 」を参照してください。	2023 年 10 月 26 日
<u>Wickr ネットワークが 間で</u> フェデレーションできるよう になりました AWS リージョ ン	Wickr ネットワークが AWS リージョン間でフェデレー トできる機能が追加されまし た。詳しくは「 <u>セキュリティ</u> <u>グループ</u> 」を参照してくださ い。	2023 年 9 月 29 日
<u>Wickr が欧州 (ロンドン) で利</u> <u>用可能に AWS リージョン</u>	Wickr が欧州 (ロンドン) で 利用可能になりました AWS リージョン。詳細について は、 <u>「リージョンの可用性</u> 」 を参照してください。	2023 年 8 月 23 日
<u>Wickr がカナダ (中部) で利用</u> <u>可能になりました AWS リー</u> <u>ジョン</u>	Wickr がカナダ (中部) で利 用可能になりました AWS リージョン。詳細について は、 <u>「リージョンの可用性</u> 」 を参照してください。	2023 年 7 月 3 日

<u>ゲストユーザー機能をプレ</u> <u>ビューできるようになりまし</u> <u>た</u>	ゲストユーザーは、Wickr ク ライアントにサインインし て、Wickr ネットワークユー ザーと共同作業できます。詳 細については、「 <u>ゲストユー</u> <u>ザー (プレビュー)</u> 」を参照し てください。	2023 年 5 月 31 日
<u>AWS Wickr が と統合され</u> <u>AWS CloudTrail、WickrGov と</u> して AWS GovCloud (米国西 部) で利用可能になりました	AWS Wickr が と統合されま した AWS CloudTrail。詳細に ついては、「 <u>AWS CloudTrai</u> Iを使用した AWS Wickr API 呼び出しのログ記録」を参照 してください。さらに、Wic kr は WickrGov として AWS GovCloud (米国西部) で利用で きます。詳細については、AW S GovCloud (US) ユーザーガ イド の「 <u>AWS WickrGov</u> 」を 参照してください。	2023 年 3 月 30 日
<u>タグ付けと複数のネットワー</u> <u>ク作成</u>	タグ付けが AWS Wickr でサ ポートされるようになりまし た。詳細については、 <u>「ネッ</u> トワークタグ」を参照してく ださい。Wickr で複数のネッ トワークを作成できるように なりました。詳しくは <u>ネット</u> ワークの作成を参照してくだ さい。	2023 年 3 月 7 日
初回リリース	Wickrアドミニストレーション ガイドの初期リリース	2022 年 11 月 28 日

リリースノート

Wickr の継続的な更新と改善を追跡できるように、最近の変更を説明するリリース通知を公開しています。

2025 年 5 月

ファイルプレビューが利用可能になりました。セキュリティグループの管理者コンソールで管理者によってファイルのダウンロードが無効になっている場合、ユーザーはメッセージングタブとファイルタブでのみサポートされているファイルのリストを表示できます。

2025 年 3 月

• 再設計された Wickr 管理者コンソールが利用可能になりました。

2024 年 10 月

Wickr がネットワークの削除をサポートするようになりました。詳細については、<u>「AWS Wickr</u>でネットワークを削除する」を参照してください。

2024 年 9 月

管理者は、Microsoft Entra (Azure AD) シングルサインオンで AWS Wickr を設定できるようになりました。詳細については、「<u>Configure AWS Wickr with Microsoft Entra (Azure AD) single sign-</u><u>on</u>」を参照してください。

2024 年 8 月

- 機能強化
 - Wickr が欧州 (チューリッヒ) で利用可能になりました AWS リージョン。

2024 年 6 月

GovCloud ユーザーがクロス境界分類とフェデレーションを使用できるようになりました。詳細については、GovCloud クロス境界分類とフェデレーション」を参照してください。

2024 年 4 月

 Wickr が読み取り受信をサポートするようになりました。詳細については、「受信の読み取り」を 参照してください。

2024 年 3 月

- グローバルフェデレーションが制限付きフェデレーションをサポートするようになりました。ここでは、制限付きフェデレーションで追加された選択したネットワークに対してのみグローバルフェデレーションを有効にできます。これは、他の Wickr ネットワークで機能します AWS リージョン。詳しくはセキュリティグループを参照してください。
- 管理者は、管理コンソールの Analytics ダッシュボードで使用状況分析を表示できるようになりました。詳細については、「分析ダッシュボード」を参照してください。

2024 年 2 月

- AWS Wickr では、最大 30 人のユーザーに Premium プランの 3 か月間の無料トライアルが提供されるようになりました。変更と制限には以下が含まれます。
 - ・無制限の管理コントロールやデータ保持など、すべての Standard および Premium プラン機能 が Premium 無料トライアルで利用可能になりました。ゲストユーザー機能は、プレミアム無料 トライアル中は利用できません。
 - ・以前の無料トライアルは利用できなくなりました。プレミアム無料トライアルをまだ使用していない場合は、既存の無料トライアルまたはスタンダードプランをプレミアム無料トライアルにアップグレードできます。詳細については、「プランの管理」を参照してください。

2023 年 11 月

- ゲスト ユーザー機能が一般提供されるようになりました。変更と追加には以下が含まれます。
 - ・ 他の Wickr ユーザーによる悪用を報告する機能。

- 管理者は、ネットワークがやり取りしたゲストユーザーのリストと月間使用回数を表示できます。
- 管理者はゲストユーザーによるネットワークとの通信をブロックできます。
- ・ ゲストユーザー向けの価格が追加されました。
- ・ 管理制御の機能強化
 - ・ ユーザーを一括削除/利用停止できます。
 - トークン更新の猶予期間を設定するための SSO 設定の追加。

2023 年 10 月

- 機能強化
 - ・ Wickr は、欧州 (フランクフルト) AWS リージョンで利用可能になりました。

2023 年 9 月

- 機能強化
 - Wickr ネットワークが AWS リージョン間でフェデレートできる機能が追加されました。詳しく はセキュリティグループを参照してください。

2023 年 8 月

- 機能強化
 - Wickr が欧州 (ロンドン) AWS リージョンで利用可能になりました。

2023 年 7 月

- 機能強化
 - Wickr は、カナダ (中部) AWS リージョンで使用可能になりました。

2023 年 5 月

- 機能強化
 - ・ ゲストユーザー向けのサポートが追加されました。詳細については、「<u>AWS Wickr ネットワー</u> <u>クのゲストユーザー</u>」を参照してください。

2023 年 3 月

- Wickr が と統合されました AWS CloudTrail。詳細については、「<u>を使用した AWS Wickr API コー</u> ルのログ記録 AWS CloudTrail」を参照してください。
- Wickr が WickrGov AWS として GovCloud (米国西部) で利用可能になりました。詳細については、AWS GovCloud (US) ユーザーガイドの「<u>AWS WickrGov</u>」を参照してください。
- Wickr がタグ付けをサポートしました。詳細については、「<u>AWS Wickr のネットワークタグ</u>」を 参照してください。Wickr で複数のネットワークを作成できるようになりました。詳細について は、「<u>ステップ1: ネットワークの構築</u>」を参照してください。

2023 年 2 月

 Wickr は Android Tactical Assault Kit (ATAK) をサポートできるようになりました。詳細について は、「<u>Wickr ネットワークダッシュボードで ATAK を有効にする</u>」を参照してください。

2023 年 1 月

シングルサインオン (SSO) は、無料トライアルとスタンダードを含むすべてのプランで設定できるようになりました。

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。