



ユーザーガイド

# AWS Elemental MediaPackage



# AWS Elemental MediaPackage: ユーザーガイド

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

Amazon の商標とトレードドレスは、Amazon 以外の製品またはサービスとの関連において、顧客に混乱を招いたり、Amazon の名誉または信用を毀損するような方法で使用することはできません。Amazon が所有しない他の商標はすべてそれぞれの所有者に帰属します。所有者は必ずしも Amazon との提携や関連があるわけではありません。また、Amazon の支援を受けているとはかぎりません。

# Table of Contents

AWS Elemental MediaPackage とは .....	1
を初めてお使いになる方向けの MediaPackage 情報 .....	1
概念と用語 .....	2
ライブのコンポーネント .....	3
VOD コンポーネント .....	4
サポートされている入力と出力 .....	4
ライブでサポートされるコーデックおよび入力タイプ .....	5
Live-to-VOD でサポートされるコーデックおよび入力タイプ .....	7
VOD でサポートされるコーデックおよび入力タイプ .....	9
MediaPackage の仕組み .....	13
ライブコンテンツの処理 .....	14
VOD コンテンツ処理 .....	18
ライブおよび VOD マニフェストのリファレンス .....	19
AWS Elemental MediaPackage の機能 .....	20
関連サービス .....	23
アクセス MediaPackage .....	24
の料金 MediaPackage .....	25
のリージョン MediaPackage .....	25
設定 .....	26
へのサインアップ AWS .....	26
にサインアップ AWS アカウント .....	26
管理者権限を持つユーザーを作成します。 .....	27
ポリシーと管理者以外のロールの作成 .....	28
(オプション) ステップ 1: Amazon の IAM ポリシーを作成する CloudFront .....	29
(オプション) ステップ 2: VOD 用の IAM ポリシーを作成する MediaPackage .....	30
ステップ 3: IAM コンソールでロールを作成する .....	33
ステップ 4: IAM コンソールからロールを引き受けるか、AWS CLI .....	35
他の AWS サービスへのアクセスを AWS Elemental MediaPackage に許可する .....	35
ステップ 1: ポリシーの作成 .....	36
ステップ 2: ロールの作成 .....	41
ステップ 3: 信頼関係の変更 .....	43
(オプション) 暗号化の設定 .....	44
(オプション) をインストールします。AWS CLI .....	45
開始方法 .....	46

ライブコンテンツの配信 .....	46
前提条件 .....	46
ステップ 1: MediaPackage にアクセスする .....	46
ステップ 2: チャンネルを作成する .....	47
ステップ 3: エンドポイントを作成する .....	48
(オプション) ステップ 4: MediaPackage のアクティビティをモニタリングする .....	48
ステップ 5: クリーンアップ .....	49
Live-to-VOD コンテンツ配信 .....	50
前提条件 .....	50
ステップ 1: MediaPackage にアクセスする .....	51
ステップ 2: ライブコンテンツを取り込む .....	51
ステップ 3: VOD アセットを抽出する .....	53
(オプション) ステップ 4: VOD コンテンツを出力する .....	54
(オプション) ステップ 5: MediaPackage のアクティビティをモニタリングする .....	58
ステップ 6: クリーンアップする .....	58
VOD コンテンツ配信 .....	60
前提条件 .....	60
ステップ 1: MediaPackage にアクセスする .....	60
ステップ 2: パッケージンググループの作成 .....	61
ステップ 3: パッケージング設定を作成する .....	61
ステップ 4: アセットを作成する .....	62
ステップ 5: 再生 URL を指定する .....	63
(オプション) ステップ 6: MediaPackage のアクティビティをモニタリングする .....	64
ステップ 7: クリーンアップする .....	64
ライブコンテンツの配信 .....	66
チャンネルの使用 .....	66
チャンネルの作成 .....	67
チャンネルの詳細の表示 .....	68
チャンネルの編集 .....	69
入力 URL での認証情報の更新 .....	70
チャンネルの削除 .....	71
チャンネルへのエンドポイントの追加 .....	71
エンドポイントの使用 .....	72
エンドポイントの作成 .....	72
チャンネルに関連付けられたすべてのエンドポイントの表示 .....	105
単一のエンドポイントの表示 .....	106

エンドポイントの編集 .....	106
エンドポイントの削除 .....	107
エンドポイントのプレビュー .....	108
VOD コンテンツの配信 .....	109
パッケージグループの使用 .....	109
パッケージグループの作成 .....	110
パッケージグループの詳細の表示 .....	111
パッケージンググループの編集 .....	111
パッケージンググループの削除 .....	112
パッケージンググループへのパッケージング設定の追加 .....	113
パッケージング設定の使用 .....	113
パッケージング設定の作成 .....	114
パッケージ設定に関する詳細の表示 .....	132
パッケージング設定の編集 .....	134
パッケージング設定の削除 .....	134
アセットの使用 .....	134
アセットの取り込み .....	135
アセットの詳細の表示 .....	139
アセットの編集 .....	139
アセットの削除 .....	139
Live-to-VOD アセットの作成 .....	141
Live-to-VOD の要件 .....	141
Live-to-VOD の仕組み .....	142
収集ジョブの使用 .....	143
収集ジョブの作成 .....	144
収集ジョブの詳細の表示 .....	147
収集ジョブの編集 .....	147
収集ジョブの削除 .....	147
MediaPackage の機能 .....	149
CDN 認証 .....	149
仕組み .....	149
CDN 認証の設定 .....	150
CDN ヘッダー値の更新 .....	155
コンテンツの暗号化と DRM .....	155
制限事項と要件 .....	155
適切な SPEKE バージョンを選択する .....	156

SPEKE のデプロイ .....	159
コンテンツキーで使用する証明書の準備と管理 .....	159
キーローテーションの動作について .....	161
SPEKE バージョン 2.0 のプリセット .....	161
DASH マニフェストの処理 .....	165
複数期間 DASH .....	167
圧縮された DASH マニフェスト .....	171
DASH マニフェストのセグメントテンプレート形式 .....	174
マニフェストでのフィルタリング .....	180
マニフェストフィルタの使用 .....	180
マニフェストフィルタクエリパラメータ .....	183
マニフェストフィルタリングの例 .....	189
HLS および CMAF マニフェストの特別な条件 .....	190
エラー状態 .....	190
メタデータのパススルー .....	192
ID3 メタデータに関する考慮事項 .....	193
KLV メタデータに関する考慮事項 .....	194
レンディショングループ .....	195
レンディショングループの使用が適切であるケース .....	195
レンディショングループの使用が適切でないケース .....	196
SCTE-35 メッセージ .....	197
MediaPackage での SCTE-35 の設定 .....	198
使用方法 .....	199
EXT-X-DATERANGE 広告マーカ .....	200
タイムシフト表示 .....	203
開始/終了パラメータのルール .....	205
トリックプレイ再生 .....	207
I フレームのプレイリストを使用してトリックプレイ再生を有効にする .....	208
イメージメディアプレイリストを使用してトリックプレイ再生を有効にする .....	209
セキュリティ .....	212
データ保護 .....	213
DRM の実装 .....	214
CDN 認証の実装 .....	214
Identity and Access Management .....	214
対象者 .....	215
アイデンティティを使用した認証 .....	215

ポリシーを使用したアクセスの管理 .....	219
が IAM と AWS Elemental MediaPackage 連携する方法 .....	222
アイデンティティベースポリシーの例 .....	230
のシークレットのポリシー例 AWS Secrets Manager .....	233
サービス間での不分別な代理処理の防止 .....	235
トラブルシューティング .....	236
詳細はこちら .....	238
サービスリンクロールの使用 .....	239
ロギングとモニタリング .....	241
Amazon CloudWatch アラーム .....	242
AWS CloudTrail ログ .....	242
AWS Elemental MediaPackage アクセスログ .....	242
AWS Trusted Advisor .....	242
コンプライアンス検証 .....	243
耐障害性 .....	244
インフラストラクチャセキュリティ .....	244
ロギングとモニタリング .....	246
CloudWatch メトリクスによるモニタリング .....	247
ライブコンテンツ用のメトリクス .....	248
VOD コンテンツ用メトリクス .....	255
CloudWatch イベントによるモニタリング .....	259
AWS Elemental MediaPackage イベント .....	260
イベント通知の作成 .....	267
を使用した AWS Elemental MediaPackage API コールのログ記録 AWS CloudTrail .....	268
AWS Elemental MediaPackage の情報 CloudTrail .....	269
AWS Elemental MediaPackage ログファイルエントリについて .....	270
アクセスのログ記録 .....	272
CloudWatch にログを発行するためのアクセス許可 .....	272
アクセスログの作成の有効化 .....	272
アクセスログの作成の無効化 .....	274
アクセスログの形式 .....	275
アクセスログを読み取る .....	278
マニフェストの更新時間のモニタリング .....	279
XMediaPackage-マニフェスト-最後のシーケンス .....	279
XMediaPackage-Manifest-Last-Updated .....	279
マニフェストの例 .....	279

ワークフローモニター .....	286
ワークフローモニターのコンポーネント .....	288
サポートされる サービス .....	288
ワークフローモニターの設定 .....	289
ワークフローモニターの使用 .....	308
リソースのタグ付け .....	310
タグの制限 .....	310
タグの管理 .....	310
CDN の使用 .....	312
ディストリビューションの作成 .....	313
Amazon から CloudFront .....	313
ディストリビューションを表示する .....	313
ディストリビューションを編集する .....	314
ディストリビューションを削除する .....	314
クォータ .....	315
ライブコンテンツのクォータ .....	315
ライブのソフトクォータ .....	315
ライブのハードクォータ .....	316
VOD コンテンツのクォータ .....	318
VOD のソフトクォータ .....	318
VOD のハードクォータ .....	319
関連情報 .....	321
ドキュメント履歴 .....	323
以前の更新 .....	335
AWS 用語集 .....	338
.....	CCCXXix



# AWS Elemental MediaPackage とは

AWS Elemental MediaPackage (MediaPackage) は、AWS クラウドで実行される just-in-time 動画パッケージおよび発信サービスです。を使用すると MediaPackage、さまざまな再生デバイスやコンテンツ配信ネットワーク (CDNs) に、安全性、拡張性、信頼性に優れたビデオストリームを提供できます。

MediaPackage は、視聴者にブロードキャストグレードの表示エクスペリエンスを提供しながら、コンテンツを柔軟に制御および保護できます。さらに、の組み込みの耐障害性とスケーラビリティ MediaPackage により、適切な量のリソースが適切なタイミングで確保され、手動による介入は必要ありません。

## トピック

- [を初めてお使いになる方向けの MediaPackage 情報](#)
- [概念と用語](#)
- [サポートされている入力と出力](#)
- [MediaPackage の仕組み](#)
- [AWS Elemental MediaPackage の機能](#)
- [関連サービス](#)
- [アクセス MediaPackage](#)
- [の料金 MediaPackage](#)
- [のリージョン MediaPackage](#)

## を初めてお使いになる方向けの MediaPackage 情報

を初めて使用する場合は MediaPackage、まず以下のセクションを読むことをお勧めします。

- [概念と用語](#)
- [MediaPackage の仕組み](#)
- [AWS Elemental MediaPackage の機能](#)
- [AWS Elemental MediaPackage の開始方法](#)

## 概念と用語

AWS Elemental MediaPackage (MediaPackage) には、次のコンポーネントが含まれています。

### Just-in-time パッケージング

MediaPackage は just-in-time パッケージング (JITP) を実行します。再生デバイスがコンテンツをリクエストすると、はライブビデオストリームを MediaPackage 動的にカスタマイズし、リクエスト元のデバイスと互換性のある形式でマニフェストを作成します。

### 配信サービス

MediaPackage メディアコンテンツ配信の配信場所であるため、は発信元サービスと見なされません。

### パッケージ

パッケージは、各種のプレーヤーからのアクセスに合わせて出力ストリームを準備します。パッケージタイプは、がエンドポイントから MediaPackage 配信するストリーミング形式 (Apple HLS、DASH-ISO、Microsoft Smooth Streaming、または Common Media Application Format [CMAF]) を指定します。追加のパッケージ設定には、バッファと更新の所要期間やマニフェストタグの処理手順などが含まれます。

パッケージはエンドポイントの一部です。パッケージは、エンドポイントごとに1つに限られます。同じコンテンツに対して複数の異なるパッケージタイプを使用するには、チャンネルで複数のエンドポイントを作成します。

### ソースコンテンツ

ソースコンテンツは、MediaPackage が取り込むライブストリームとビデオファイルです。

- ライブ動画の場合、ソースコンテンツは などのアップストリームエンコーダーから取得されません。AWS Elemental MediaLive は HLS ソースコンテンツ MediaPackage をサポートします。
- ビデオオンデマンド (VOD) の場合、ソースコンテンツはAWSアカウントの Amazon Simple Storage Service (Amazon S3) バケットにあります。は HLS および MP4 (.smil マニフェスト形式) コンテンツ MediaPackage をサポートしています。

### ストリーム

ストリームとは、のコンテンツ入出力を指します MediaPackage。

ライブワークフローの場合、アップストリームエンコーダーはライブストリームを MediaPackage への入力としてチャンネルに送信します。ダウンストリームデバイスがコンテンツ

の再生をリクエストすると、ストリームを MediaPackage 動的にパッケージ化し (パッケージタイプ の指定、暗号化の追加、トラック出力の設定を含む)、エンドポイントの出力としてリクエスト元のデバイスに配信します。エンドポイントは複数のストリームを生成できます。

VOD ワークフローの場合、は Amazon S3 からファイルベースのコンテンツを MediaPackage プルします。ライブワークフローと同様に、ダウンストリームデバイスがコンテンツの再生をリクエストすると、はストリームを MediaPackage 動的にパッケージ化し、アセットリソースの出力としてリクエスト元のデバイスに配信します。

## Track

トラックは出力コンテンツストリームを構成します。MediaPackage 選択したビデオ、オーディオ、字幕または字幕トラックが出力ストリームに含まれます。ストリームは、これらのトラックを (直接または CDN 経由で) プレーヤーに配信します。プレーヤーは、プレーヤーロジックまたはネットワーク条件 (使用可能な帯域幅など) に基づいてトラックを再生します。

## ライブのコンポーネント

のライブワークフローには、次のコンポーネントが適用されます MediaPackage。

### チャンネル

チャンネルは、へのコンテンツストリームのエントリポイントを表します MediaPackage。AWS Elemental MediaLive などのアップストリームエンコーダーは、チャンネルにコンテンツを送信します。がコンテンツストリーム MediaPackage を受信すると、コンテンツをパッケージ化し、チャンネルで作成したエンドポイントからストリームを出力します。着信するアダプティブビットレート (ABR) ストリームのセットごとに 1 つのチャンネルがあります。

### エンドポイント

エンドポイントは、チャンネルの一部として MediaPackage のパッケージ化面を担当します。チャンネルでエンドポイントを作成するときに、出力ストリームで使用するストリーミング形式、パッケージングパラメータ、および機能を指定します。ダウンストリームデバイスは、エンドポイントに対してコンテンツをリクエストします。チャンネルは複数のエンドポイントを持つことができます。

### 収集ジョブ

ハーベストジョブは、ライブコンテンツストリームから VOD アセットを抽出するために作成するタスクです。収集ジョブは、VOD アセットの開始時刻と終了時刻、および がアセット MediaPackage を保存する場所を定義します。ジョブが実行されると、は指定した時刻の HLS

クリップ MediaPackage を作成します。このクリップは、選択した Amazon S3 バケットに VOD アセットとして保存されます。MediaPackage の VOD 機能を使用して、アセットをエンドユーザーに提供できます。

## VOD コンポーネント

の VOD ワークフローには、次のコンポーネントが適用されます MediaPackage。

### アセット

アセットは、ファイルベースのコンテンツのエントリポイントを . MediaPackage MediaPackage uses に表し、アセット内の情報を使用して Amazon S3 からソースコンテンツを見つけて取り込みます。アセットを作成するときは MediaPackage、1 つ以上のパッケージング設定 を保持するパッケージンググループ にアセットを関連付けます。アセットとパッケージング設定のそれぞれの組み合わせで、再パッケージ化されたコンテンツ再生用の 1 つの URL が利用できます。各アセットは、1 つのパッケージンググループ内にあるすべてのパッケージング設定と関連付けられています。

### パッケージング設定

パッケージング設定では、MediaPackage でソースコンテンツがビューワーにどのようにフォーマット、暗号化、配信されるかが定義されます。パッケージ設定には、ストリームの選択、暗号化、セグメントの時間と組み合わせなどの設定、および 1 つまたは複数の HLS、DASH、MSS、CMAF のマニフェスト定義が含まれています。

### パッケージンググループ

パッケージンググループは、1 つ以上のパッケージング設定のセットです。グループは、複数のアセットに関連付けることができるため、グループを使用すると、複数のパッケージンググループを効率的に複数のアセットに関連付けることができます。

## サポートされている入力と出力

このセクションでは、AWS Elemental MediaPackage でライブおよびビデオオンデマンド (VOD) コンテンツに対してサポートされる入力タイプ、入力コーデック、出力コーデックについて説明しています。

### トピック

- [ライブでサポートされるコーデックおよび入力タイプ](#)

- [Live-to-VOD でサポートされるコーデックおよび入力タイプ](#)
- [VOD でサポートされるコーデックおよび入力タイプ](#)

## ライブでサポートされるコーデックおよび入力タイプ

以下のセクションでは、ライブストリーミングコンテンツに対してサポートされる入力タイプおよびコーデックについて説明します。

### サポートされている入力タイプ

これらは、ライブコンテンツ用に が MediaPackage サポートする入力タイプです。

MediaPackage 入力タイプ	ユースケース
HLS	<p>HTTPS プロトコルを使用して外部ソースあるいはエンコーダー (AWS Elemental MediaLive など) から HLS ストリームをプッシュします。</p> <p>その他の要件:</p> <ul style="list-style-type: none"> <li>• 入力は WebDAV を介し、ダイジェスト認証を使用する必要があります。</li> <li>• メディアセグメントは暗号化されていないことが必要です。</li> <li>• ストリームには、Mux 処理された動画と音声トラック、あるいは Mux 処理されていないトラックのいずれかを含めることができます。</li> <li>• 入力には少なくとも 1 つのビデオトラックが含まれている必要があります。MediaPackage は、ビデオトラックを含まない入力をサポートしていません。</li> </ul>

### サポートされる入力コーデック

これらは、ソースコンテンツストリーム用に が MediaPackage サポートするビデオ、オーディオ、字幕のコーデックです。

メディアコンテナ	ビデオコーデック	オーディオコーデック	字幕/キャプション形式
<ul style="list-style-type: none"> <li>• 動画: TS</li> <li>• 音声: TS、AAC、AC3、あるいは EC3</li> </ul>	<ul style="list-style-type: none"> <li>• H.264 (AVC)</li> <li>• H.265 (HEVC) と HDR-10 のサポート</li> </ul>	<ul style="list-style-type: none"> <li>• AAC</li> <li>• ドルビーデジタル</li> <li>• ドルビーデジタルプラス</li> </ul>	<ul style="list-style-type: none"> <li>• WebVTT</li> <li>• CEA-608 と CEA-708 のクローズドキャプション</li> </ul>

## サポートされる出力コーデック

これらは、ライブコンテンツを配信する際に MediaPackage がサポートするビデオ、オーディオ、字幕のコーデックです。

[エンドポイントタイプ]	マニフェスト形式	メディアコンテナ	ビデオコーデック	オーディオコーデック	字幕/キャプション形式
Apple HLS	HLS	<ul style="list-style-type: none"> <li>• 動画: TS</li> <li>• 音声: TS または AAC</li> </ul>	<ul style="list-style-type: none"> <li>• H.264 (AVC)</li> <li>• H.265 (HEVC) と HDR-10 のサポート</li> </ul>	<ul style="list-style-type: none"> <li>• AAC</li> <li>• ドルビーデジタル</li> <li>• ドルビーデジタルプラス</li> </ul>	<ul style="list-style-type: none"> <li>• WebVTT</li> <li>• CEA-608 と CEA-708 のクローズドキャプション</li> </ul>
DASH-ISO	MPEG-DASH	MP4	<ul style="list-style-type: none"> <li>• H.264 (AVC)</li> <li>• H.265 (HEVC) と HDR-10 のサポート</li> </ul>	<ul style="list-style-type: none"> <li>• AAC</li> <li>• ドルビーデジタル</li> <li>• ドルビーデジタルプラス</li> </ul>	<ul style="list-style-type: none"> <li>• EBU-TT</li> <li>• CEA-608 と CEA-708 のクローズドキャプション</li> </ul>
Microsoft Smooth	MSS	MP4	<ul style="list-style-type: none"> <li>• H.264 (AVC)</li> <li>• H.265 (HEVC) と</li> </ul>	<ul style="list-style-type: none"> <li>• AAC</li> <li>• ドルビーデジタル</li> </ul>	DFXP

[エンドポイントタイプ]	マニフェスト形式	メディアコンテナ	ビデオコーデック	オーディオコーデック	字幕/キャプション形式
			HDR-10 のサポート	• ドルビーデジタルプラス	
CMAF	HLS	CMAF	<ul style="list-style-type: none"> <li>• H.264 (AVC)</li> <li>• H.265 (HEVC) と HDR-10 のサポート</li> </ul>	<ul style="list-style-type: none"> <li>• AAC</li> <li>• ドルビーデジタル</li> <li>• ドルビーデジタルプラス</li> </ul>	<ul style="list-style-type: none"> <li>• WebVTT</li> <li>• CEA-608 と CEA-708 のクローズドキャプション</li> </ul>

## Live-to-VOD でサポートされるコーデックおよび入カタイプ

以下のセクションでは、AWS Elemental MediaPackage でストリーミングコンテンツから収集された Live-to-VOD アセットでサポートされる入カタイプとコーデックについて説明します。

### サポートされている入カタイプ

これらは、Live-to-VOD アセットに対してが MediaPackage サポートする入カタイプです。

MediaPackage 入カタイプ	ユースケース
HLS	<p>で MediaPackage ライブ HLS または DASH エンドポイントの一部を抽出し、Live-to-VOD アセットとして保存します。</p> <p>その他の要件:</p> <ul style="list-style-type: none"> <li>• エンドポイントには、収集可能な live-to-VOD アセットの最大長を決定するスタートオーバーウィンドウが定義されている必要があります。</li> <li>• ストリームには、Mux 処理された動画と音声トラック、あるいは Mux 処理されていな</li> </ul>

MediaPackage 入力タイプ	ユースケース
	<p>いトラックのいずれかを含めることができます。</p> <ul style="list-style-type: none"> <li>入力には少なくとも 1 つのビデオトラックが含まれている必要があります。MediaPackage は、ビデオトラックを含まない入力をサポートしていません。</li> </ul>

## サポートされる入力コーデック

これらは、Live-to-VOD アセット用に が MediaPackage サポートするビデオ、オーディオ、字幕のコーデックです。

メディアコンテナ	ビデオコーデック	オーディオコーデック	字幕/キャプション形式
<ul style="list-style-type: none"> <li>動画: TS</li> <li>音声: TS、AAC、AC3、あるいは EC3</li> </ul>	<ul style="list-style-type: none"> <li>H.264 (AVC)</li> <li>H.265 (HEVC) と HDR-10 のサポート</li> </ul>	<ul style="list-style-type: none"> <li>AAC</li> <li>ドルビーデジタル</li> <li>ドルビーデジタルプラス</li> </ul>	<ul style="list-style-type: none"> <li>WebVTT</li> <li>CEA-608 と CEA-708 のクローズドキャプション</li> </ul>

## サポートされる出力コーデック

以下は、Live-to-VOD アセットを Amazon S3 バケットに保存するとき が MediaPackage サポートするビデオ、オーディオ、字幕のコーデックです。エンドポイントは、明確な (非暗号化の) または暗号化された、DASH または HLS コンテンツのどちらかを提供する必要があります。

[エンドポイントタイプ]	マニフェスト形式	メディアコンテナ	ビデオコーデック	オーディオコーデック	字幕/キャプション形式
Apple HLS	HLS	<ul style="list-style-type: none"> <li>動画: TS</li> <li>音声: TS または AAC</li> </ul>	<ul style="list-style-type: none"> <li>H.264 (AVC)</li> <li>H.265 (HEVC) と</li> </ul>	<ul style="list-style-type: none"> <li>AAC</li> <li>ドルビーデジタル</li> </ul>	<ul style="list-style-type: none"> <li>WebVTT</li> <li>CEA-608 と CEA-708</li> </ul>



[エンドポイントタイプ]	マニフェスト形式	メディアコンテナ	ビデオコーデック	オーディオコーデック	字幕/キャプション形式
			HDR-10 のサポート	<ul style="list-style-type: none"> <li>ドルビーデジタルプラス</li> </ul>	のクローズドキャプション
DASH-ISO	MPEG-DASH	MP4	<ul style="list-style-type: none"> <li>H.264 (AVC)</li> <li>H.265 (HEVC) と HDR-10 のサポート</li> </ul>	<ul style="list-style-type: none"> <li>AAC</li> <li>ドルビーデジタル</li> <li>ドルビーデジタルプラス</li> </ul>	<ul style="list-style-type: none"> <li>EBU-TT</li> <li>CEA-608 と CEA-708 のクローズドキャプション</li> </ul>

## VOD でサポートされるコーデックおよび入カタイプ

以下のセクションでは、ファイルベースのビデオオンデマンド (VOD) コンテンツに対してサポートされる入カタイプおよびコーデックについて説明します。

### サポートされている入カタイプ

これらは、 が VOD コンテンツで MediaPackage サポートする入カタイプです。

MediaPackage 入カタイプ	ユースケース
HLS	<p>安全な接続の有無にかかわらず、Amazon S3 バケットから HLS ストリームセットをプルします。</p> <p>その他の要件:</p> <ul style="list-style-type: none"> <li>メディアセグメントは暗号化されていないことが必要です。</li> <li>ストリームには、Mux 処理された動画と音声トラック、あるいは Mux 処理されていないトラックのいずれかを含めることができます。</li> </ul>

MediaPackage 入力タイプ	ユースケース
	<ul style="list-style-type: none"> <li>入力には少なくとも 1 つのビデオトラックが含まれている必要があります。MediaPackage は、ビデオトラックを含まない入力をサポートしていません。</li> </ul>
SMIL	<p>安全な接続の有無にかかわらず、Amazon S3 バケットから .smil マニフェストで参照される MP4 ストリームセットをプルします。.smil マニフェストの詳細については、「<a href="#">.smil マニフェストでの要件</a>」を参照してください。</p> <p>その他の要件:</p> <ul style="list-style-type: none"> <li>MP4 コンテナは断片化されていない。</li> <li>メディアセグメントは暗号化されていないことが必要です。</li> <li>ストリームには、Mux 処理された動画と音声トラック、あるいは動画トラックのいずれかを含めることができます。</li> <li>各ストリームでは、タイムベースを等しくする必要があります。</li> </ul>

## サポートされる入力コーデック

これらは、ファイルベースのソースコンテンツに対して MediaPackage サポートするビデオ、オーディオ、字幕のコーデックです。

入力タイプ	メディアコンテナ	ビデオコーデック	オーディオコーデック	字幕/キャプション形式
HLS	<ul style="list-style-type: none"> <li>動画: TS</li> <li>音声: TS、AAC、AC3、あるいは EC3</li> </ul>	<ul style="list-style-type: none"> <li>H.264 (AVC)</li> <li>H.265 (HEVC) と HDR-10 のサポート</li> </ul>	<ul style="list-style-type: none"> <li>AAC</li> <li>ドルビーデジタル</li> </ul>	<ul style="list-style-type: none"> <li>WebVTT</li> <li>CEA-608 と CEA-708 のクローズドキャプション</li> </ul>

入カタイプ	メディアコンテナ	ビデオコーデック	オーディオコーデック	字幕/キャプション形式
			<ul style="list-style-type: none"> <li>ドルビーデジタルプラス</li> </ul>	
SMIL	MP4 (断片化なし)	<ul style="list-style-type: none"> <li>H.264 (AVC)</li> <li>H.265 (HEVC) と HDR-10 のサポート</li> </ul>	<ul style="list-style-type: none"> <li>AAC</li> <li>ドルビーデジタル</li> <li>ドルビーデジタルプラス</li> </ul>	SRT

## サポートされる出力コーデック

これらは、が VOD コンテンツを配信するために MediaPackage サポートするビデオ、オーディオ、字幕のコーデックです。

[エンドポイントタイプ]	マニフェスト形式	メディアコンテナ	ビデオコーデック	オーディオコーデック	字幕/キャプション形式
Apple HLS	HLS	<ul style="list-style-type: none"> <li>動画: TS</li> <li>音声: TS、AAC、A3、あるいは EC3</li> </ul>	<ul style="list-style-type: none"> <li>H.264 (AVC)</li> <li>H.265 (HEVC) と HDR-10 のサポート</li> </ul>	<ul style="list-style-type: none"> <li>AAC</li> <li>ドルビーデジタル</li> <li>ドルビーデジタルプラス</li> </ul>	<ul style="list-style-type: none"> <li>WebVTT</li> <li>CEA-608 と CEA-708 のクローズドキャプション</li> </ul>
DASH-ISO	MPEG-DASH	MP4	<ul style="list-style-type: none"> <li>H.264 (AVC)</li> <li>H.265 (HEVC) と HDR-10 のサポート</li> </ul>	<ul style="list-style-type: none"> <li>AAC</li> <li>ドルビーデジタル</li> <li>ドルビーデジタルプラス</li> </ul>	<ul style="list-style-type: none"> <li>EBU-TT</li> <li>CEA-608 と CEA-708 のクローズドキャプション</li> </ul>

[エンドポイントタイプ]	マニフェスト形式	メディアコンテナ	ビデオコーデック	オーディオコーデック	字幕/キャプション形式
Microsoft Smooth	MSS	MP4	<ul style="list-style-type: none"> <li>H.264 (AVC)</li> <li>H.265 (HEVC) と HDR-10 のサポート</li> </ul>	<ul style="list-style-type: none"> <li>AAC</li> <li>ドルビーデジタル</li> <li>ドルビーデジタルプラス</li> </ul>	DFXP
CMAF	HLS	CMAF	<ul style="list-style-type: none"> <li>H.264 (AVC)</li> <li>H.265 (HEVC) と HDR-10 のサポート</li> </ul>	<ul style="list-style-type: none"> <li>AAC</li> <li>ドルビーデジタル</li> <li>ドルビーデジタルプラス</li> </ul>	<ul style="list-style-type: none"> <li>WebVTT</li> <li>CEA-608 と CEA-708 のクローズドキャプション</li> </ul>

## .smil マニフェストでの要件

VOD MP4 アセットを AWS Elemental MediaPackage に送信する場合は、.smil マニフェストを含める必要があります。.smil マニフェストは、アセット内のすべてのファイルのラッパーとして機能する XML ファイルで、どの MP4s が単一のアセットの一部であるかを MediaPackage に伝えます。

### リソース

- .smil マニフェストの作成に関するガイダンスについては、[「AWS Elemental MediaPackage VOD を使用した .smil」](#) ( ブログ ) を参照してください。
- SMIL (Synchronized Multimedia Integration Language) に関する一般的な情報については、[SMIL 3.0 仕様](#) を参照してください。

MediaPackage は、.smil マニフェストで次の属性をサポートします。

### 属性

- audioName – オーディオトラックの名前 (English 2 など)。

- `includeAudio` - オーディオトラックを含めるかどうかを示すブール値。この属性には、定義された言語と同じ数の値が含まれている必要があります。指定しない場合、すべてのトラックがデフォルトで `true` になります。
- `src` または `name` - マニフェストの場所に相対的なテキストストリームまたは動画ファイルの名前またはソースのいずれかです。
- `subtitleName` - 字幕名 (English など)。
- `systemLanguage` または `language` - システム言語 (eng など)。

## Example .smil マニフェスト

以下は .smil マニフェストの例です。

```
<?xml version="1.0" encoding="utf-8"?>
<smil>
  <body>
    <alias value="Example"/>
    <switch>
      <video name="example_360.mp4" systemLanguage="eng, fra, spa"
audioName="English, French, Spanish" includeAudio="true, true, true"/>
      <video name="example_480.mp4" systemLanguage="eng" audioName="English 2"
includeAudio="false"/>
      <textstream src="example_subs_eng.srt" systemLanguage="eng"
subtitleName="English" includeAudio="false"/>
      <textstream src="example_subs_fra.srt" systemLanguage="fra"
subtitleName="French" includeAudio="false"/>
      <textstream src="example_subs_spa.srt" systemLanguage="spa"
subtitleName="Spanish" includeAudio="false"/>
    </switch>
  </body>
</smil>
```

## MediaPackage の仕組み

AWS Elemental MediaPackage (MediaPackage) は、just-in-time 形式変換を使用して、単一のソースからさまざまな再生デバイスまたはコンテンツ配信ネットワーク over-the-top (CDNs)。

以下のセクションでは、MediaPackage の仕組みについて説明します。

### トピック

- [ライブコンテンツの処理](#)
- [VOD コンテンツ処理](#)
- [ライブおよび VOD マニフェストのリファレンス](#)

## ライブコンテンツの処理

ライブコンテンツの処理フローでは、エンコーダーはライブ HLS ストリームを に送信し MediaPackage し MediaPackage、コンテンツをパッケージ化し、ダウンストリームデバイスからの再生リクエストに応じてフォーマットします。

以下のセクションでは、ライブ処理の流れについて説明します。

### トピック

- [一般的な MediaPackage ライブ処理フロー](#)
- [ライブ入力冗長の AWS Elemental MediaPackage 処理の流れ](#)

### 一般的な MediaPackage ライブ処理フロー

以下に、 のライブコンテンツの一般的なフローの概要を示します MediaPackage。

1. アップストリームエンコーダー ( などAWS Elemental MediaLive) は、WebDAV 経由でダイジェスト認証を使用して HLS ライブストリームを MediaPackage チャンネル入力 URL に送信し、チャンネルのアクセス認証情報 ( で指定) を含めます MediaPackage。入力冗長を使用している場合、エンコーダーは 2 つの同一の HLS ライブストリームを に送信します。1 MediaPackage つはチャンネルの各入力 URL です。MediaPackage は、1 つの入力 URL からのストリームをソースコンテンツとして使用します。がアクティブな入力 URL でのコンテンツの受信 MediaPackage を停止すると、ソースコンテンツの他の入力 URL に自動的に切り替わります。また、AWS は、リソースをスケールアップ/ダウンして着信トラフィックに対処します。

詳細については、「[ライブ入力冗長の AWS Elemental MediaPackage 処理の流れ](#)」を参照してください。

#### Note

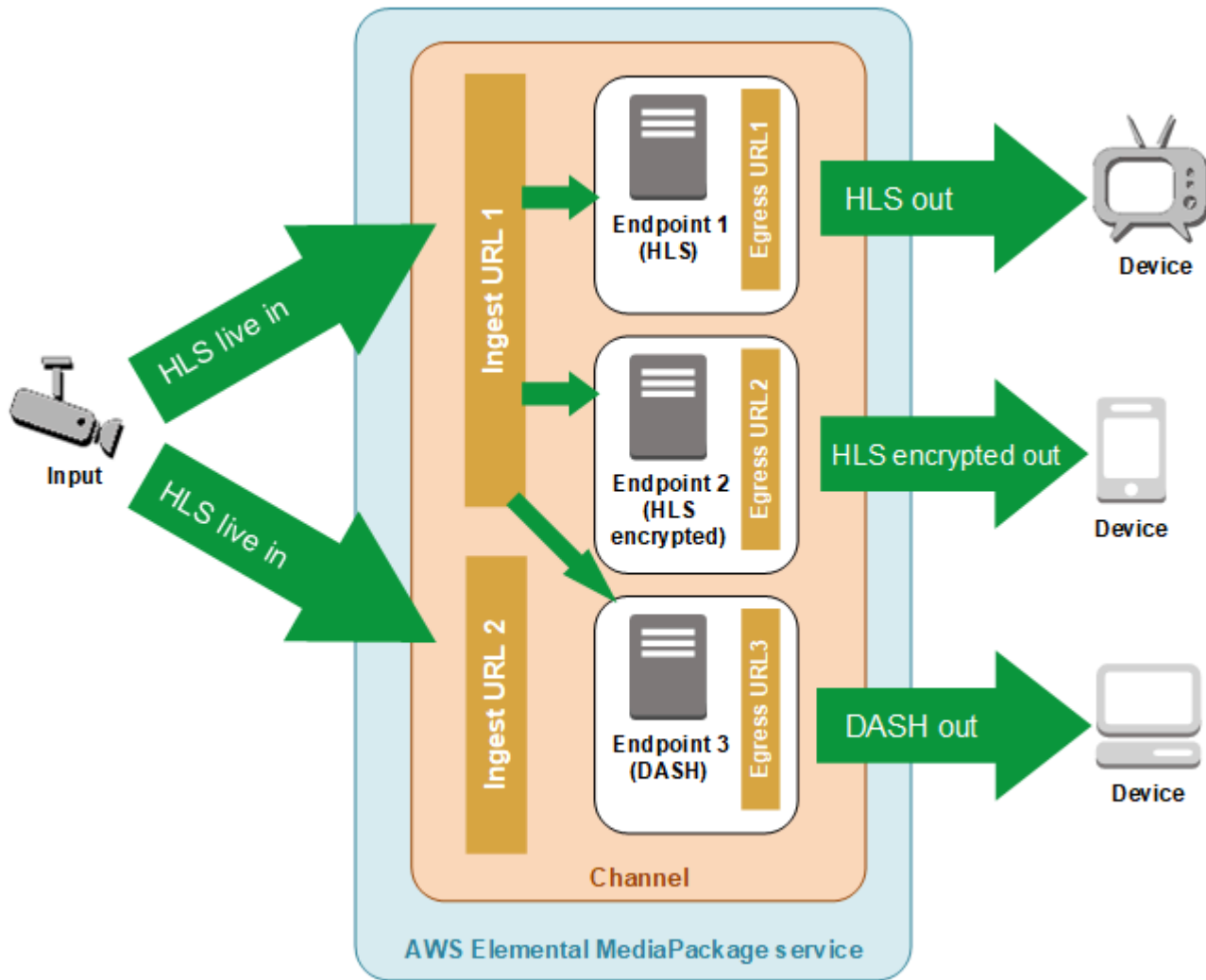
タイムシフト表示などの機能のサポートを可能にするために、 は受信したすべてのコンテンツを期間限定で MediaPackage 保存します。この保存されたコンテンツは、エンドポイントで定義されているスタートオーバーウィンドウ内にある場合にのみ再生できます。

スタートオーバーウィンドウ外にある場合、またはエンドポイントでウィンドウが定義されていない場合、保存されたコンテンツは再生できません。詳細については、「[AWS Elemental MediaPackage のタイムシフト表示のリファレンス](#)」を参照してください。

2. ダウンストリームデバイスは、エンドポイント出力 URL MediaPackage を介して からコンテンツをリクエストします。ダウンストリームデバイスは、動画プレイヤーまたは CDN のいずれかです。出力 URL は、ストリーミング形式別 (Apple HLS、DASH-ISO、Microsoft Smooth Streaming、CMAF のいずれか) のエンドポイントに関連付けられています。
3. がダウンストリームデバイスから再生リクエスト MediaPackage を受信すると、エンドポイントで指定した設定に従ってストリームが動的にパッケージ化されます。パッケージ化には、暗号化の追加、オーディオ、ビデオ、サブタイトル/キャプションのトラック出力の設定などが含まれます。
4. MediaPackage は、HTTPS 経由で出カストリームをリクエスト元のデバイスに配信します。入力の場合と同様に、AWS でリソースをスケールアップ/ダウンしてトラフィックの変化に対処します。
5. MediaPackage は、Amazon を介してアクティビティを記録します CloudWatch。コンテンツリクエストの数や、 が受信または配信 MediaPackage したコンテンツの量などの情報を表示できます。で MediaPackage メトリクスを表示する方法については CloudWatch、「」を参照してください [Amazon CloudWatch メトリクス AWS Elemental MediaPackage によるモニタリング](#)。

コンテンツの入力および出カプロセスを通じて、 は、視聴者にとって問題になる前に、潜在的なインフラストラクチャ障害 MediaPackage を検出して軽減します。

このプロセスの概要は次の図のとおりです。



## ライブ入力冗長の AWS Elemental MediaPackage 処理の流れ

AWS Elemental MediaPackage で入力冗長を実現するには、MediaPackage でチャンネルの個別の入力 URL に 2 つのストリームを送信します。2 つのストリームの片方がそのエンドポイントのコンテンツのプライマリでアクティブなソースになり、もう片方はパッシブにコンテンツの受信を続けます。がアクティブなストリームからのコンテンツの受信 MediaPackage を停止すると、コンテンツの再生が中断されないように、他の入力ストリームに切り替えます。

MediaPackage でを使用する場合 AWS Elemental MediaLive (例: )、入力冗長のフローは次のとおりです。

1. 「」で説明されているように MediaPackage、でチャンネルを作成します[チャンネルの作成](#)。MediaPackage がチャンネルをプロビジョンすると、チャンネルに 2 つの入力 URL が作成されます。入力冗長を使用していない場合は、いずれかの入力 URL にストリームを送信できます。必ずしも両方の URL にコンテンツを送信する必要はありません。



**Note**

入力冗長が利用可能になると、は既存のチャンネルに 2 番目の入力 URL MediaPackage を追加し、既存の URL を新しい形式に更新しました。コンテンツ入力には新旧の URL のいずれかを使用できます。

- 「」の説明 MediaPackage に従って、でエンドポイントを作成します [エンドポイントの作成](#)。

**Important**

短い出力セグメントを使用する場合、再生デバイスによっては、が入力 MediaPackage を切り替えるとバッファリングが表示されることがあります。バッファリングはエンドポイントの時間遅延機能を使用して軽減できます。時間遅延を使用すると、コンテンツの end-to-end 配信にレイテンシーが生じることに注意してください。時間遅延を有効にする方法の詳細については、「[エンドポイントの作成](#)」を参照してください。

- AWS Elemental MediaLive に入力とチャンネルを作成し、MediaLive のチャンネルに MediaPackage 出力グループを追加します。詳細については、AWS Elemental MediaLive ユーザーガイドの「[Creating a Channel from Scratch](#)」を参照してください。

AWS Elemental MediaLive で HLS グループを使用する場合は、HLS グループの設定で、サービスで入力が受け取られない場合の入力損失時のアクションを、出力の一時停止に設定する必要があります。が入力がないときにブラックフレームまたは他のフィラーフレーム MediaLive を送信した場合、MediaPackage はセグメントが欠落しているタイミングを認識できず、その後フェイルオーバーを実行できません。での入力損失アクションの設定の詳細については MediaLive、AWS Elemental MediaLive ユーザーガイドの「[HLS グループのフィールド](#)」を参照してください。

**Important**

別のエンコーダー (ではないAWS Elemental MediaLive) を使用し、で 2 つの別々のストリームを同じチャンネルに送信する場合 MediaPackage、ストリームのエンコーダー設定とマニフェスト名は同じである必要があります。それ以外の場合は、入力冗長が正常に機能せず、入力が切り替わったときに再生が中断される可能性があります。

- AWS Elemental MediaLive のチャンネルで MediaPackage へのストリーム送信を開始します。

- MediaPackage は両方の入力 URLs でコンテンツを受け取りますが、ソースコンテンツには一度に 1 つのストリームのみが使用されます。アクティブなストリームにセグメントがない場合、は自動的に他のストリームに MediaPackage フェイルオーバーします。フェイルオーバーが再び必要になるまで、はこのストリームを MediaPackage 使用するために続行します。

入力でセグメントが欠落しているかを判断するために使用される計算式は、入力とエンドポイントのセグメントの長さに基づきます。入力でセグメントが欠落したがすぐに回復した場合、それより長いセグメント長を使用するエンドポイントでは入力を切り替えません。これにより、チャネルの異なるエンドポイントで異なる入力を使用する (1 つのエンドポイントでは切り替え、もうひとつでは切り替えない場合) ことがあります。これは正常な動作であり、コンテンツのワークフローには影響しません。

## VOD コンテンツ処理

VOD コンテンツの処理フローでは、AWS Elemental MediaPackage は Amazon S3 からファイルベースの動画コンテンツを取り込み MediaPackage、コンテンツをパッケージ化し、ダウンストリームデバイスからの再生リクエストに応じてフォーマットします。

MediaPackage での VOD コンテンツの一般的な処理の流れは以下のとおりです。

- MediaPackage アセットから、Amazon S3 バケットからソースコンテンツの取り込みを開始します。この処理には数分かかることもあります。取り込みが完了し、再生 URLs がライブになると、Amazon CloudWatch イベントを受け取ります。
- ダウンストリームデバイスは、アセットのパッケージング設定 URL MediaPackage を介してからコンテンツをリクエストします。ダウンストリームデバイスは、動画プレイヤーまたは CDN のいずれかです。URL は、ストリーミング形式別 (Apple HLS、DASH-ISO、Microsoft Smooth、CMAF のいずれか) の設定に関連付けられています。
- がダウンストリームデバイスから再生リクエスト MediaPackage を受信すると、パッケージング設定で指定した設定に従ってストリームが動的にパッケージ化されます。パッケージ化には、暗号化の追加、オーディオ、ビデオ、サブタイトル/キャプションのトラック出力の設定などが含まれます。
- MediaPackage は、HTTPS 経由で出力ストリームをリクエスト元のデバイスに配信します。入力の場合と同様に、AWS でリソースをスケールアップ/ダウンしてトラフィックの変化に対処します。
- MediaPackage は、Amazon を介してアクティビティを記録します CloudWatch。MediaPackage が配信したコンテンツリクエスト数やコンテンツ量のような情報を表示できます。での

MediaPackage VOD メトリクスの表示については CloudWatch、「」を参照してください [Amazon CloudWatch メトリクス AWS Elemental MediaPackage によるモニタリング](#)。

コンテンツの入力および出力プロセスを通じて、は、視聴者にとって問題になる前に、潜在的なインフラストラクチャ障害 MediaPackage を検出して軽減します。

## ライブおよび VOD マニフェストのリファレンス

AWS Elemental MediaPackage は、ライブおよびビデオオンデマンド (VOD) マニフェストをリクエストするデバイスに配信します。ライブマニフェストは、コンテンツが完了していないことを示します。新しいコンテンツは、再生エンドポイントを通じて継続的に利用可能になります。または、VOD マニフェストによって、プログラムが完了したこと、または今後の指定された時間に完了することが示されます。

このセクションでは、ライブマニフェストと VOD マニフェストの違いと、各マニフェストタイプをいつ MediaPackage 配信するかについて説明します。

### マニフェストのプロパティ

ライブまたは VOD を決定する、マニフェストの主なプロパティを以下に示します。

- HLS および CMAF VOD マニフェストの場合、EXT-X-ENDLIST は、ビットレートマニフェストの最後を表します。ライブマニフェストでは、このタグは存在しません。
- MPEG-DASH VOD マニフェストの場合、type="static" は、MPD プロパティ内にあります。ライブマニフェストでは、type=dynamic です。
- Microsoft Smooth VOD マニフェストの場合、IsLive は SmoothStreamingMedia 内プロパティ内にありません。ライブマニフェストでは、IsLive=TRUE です。

VOD の場合、再生デバイスのスクラバーでも、プログラムの期間が制限されていることが度々示されます。この期間は、現在のマニフェストと同じ長さです。再生リクエストで特定の再生ウィンドウを定義している場合、この期間はその再生ウィンドウと同じ長さになります。

マニフェストがライブか VOD かを判断するには、「」を参照してください [ライブおよび VOD マニフェストのリファレンス](#)。

### マニフェストが VOD の場合

MediaPackage は、プログラムのコンテンツが完了したときに VOD マニフェストを配信します。次の条件下でプログラムが完了した MediaPackage ことを検討してください。

過去の **end** パラメータがあります。

過去に設定された **end** が再生リクエストに含まれる場合、その内容は完了しています。新しいコンテンツは追加されません。MediaPackage は、ダウンストリームデバイスに静的な VOD マニフェストを提供します。

再生リクエストの開始パラメータおよび終了パラメータについては、[AWS Elemental MediaPackage のタイムシフト表示のリファレンス](#) を参照してください。

アップストリームエンコーダーによって MediaPackage に配信されるマニフェストには、**EXT-X-ENDLIST** タグが含まれます。

エンコーダーからの出力を停止すると、に送信するマニフェストに **EXT-X-ENDLIST** タグ MediaPackage が含まれます。このタグは、コンテンツが完了し、新しいコンテンツは追加されない MediaPackage ことを に伝えます。は、ダウンストリームデバイスに静的な VOD マニフェストを MediaPackage 配信します。

#### Note

1 つまたは両方のパイプラインが停止したときに AWS Elemental MediaLive チャンネルを手動で MediaPackage 停止した場合、への HLS MediaLive マニフェスト **EXT-X-ENDLIST** に を含めないでください MediaPackage。はライブマニフェストを生成するために MediaPackage 続行します。

チャンネルを停止したときに両方のパイプラインがアクティブな場合、MediaLive にはが含まれます **EXT-X-ENDLIST**。は VOD マニフェストをダウンストリームデバイスに MediaPackage 配信します。

エンコーダーから出力を再起動した場合、MediaPackage のマニフェストは再度有効になります。コンテンツの再生を再開するには、再生デバイスを更新する必要がある場合があります。

入力冗長およびアクティブのストリームエンドを使用している場合、MediaPackage は、入力の他の受信ストリームにフェイルオーバーされます。受信ストリームがいずれも終了していない限り、マニフェストは完了とマークされません。

## AWS Elemental MediaPackage の機能

MediaPackage は、次の機能をサポートしています。

## 音声

MediaPackage は、多言語のオーディオ入力と以下のオーディオコーデックをサポートしています。

- AAC ステレオ
- Dolby AC3 および E-AC3 (Dolby Digital および Dolby Digital+)

MediaPackage は、入力ソースからこれらのコーデックを受け入れ、出力ストリームに渡します。

### Important

MediaPackage はオーディオのみの入力をサポートしていません。エンコーダーからのストリーム設定には、少なくとも 1 つの動画トラックが含まれている必要があります。

## 字幕

埋め込みソースのキャプションとして CEA-608 キャプション、CEA-708 キャプション、または CEA-608 と CEA-708 の両方のキャプションを指定できます。MediaPackage は、HLS、CMAF、DASH エンドポイントのメディアセグメントでこれらのキャプションを通過し、適切なマニフェストシグナリングを生成します。

### Important

入力 HLS プレイリストには、タグをシグナリングするキャプションが含まれている必要があります。存在しない場合、対応する出力マニフェストシグナリングを生成 MediaPackage できません。

## CDN 認証

MediaPackage は、コンテンツ配信ネットワーク (CDN) 認証をサポートします。詳細については、[AWS Elemental MediaPackage での CDN 認証](#) を参照してください。

## DRM

MediaPackage は、デジタル著作権管理 (DRM) によるコンテンツ保護をサポートしています。詳細については、[AWS Elemental MediaPackage でのコンテンツの暗号化と DRM](#) を参照してください。

## HLS レンディショングループ

MediaPackage は、送受信 HLS コンテンツのレンディショングループをサポートします。出力レンディショングループの詳細については、「[AWS Elemental MediaPackage のレンディショングループのリファレンス](#)」を参照してください。

### Live to VOD

収集ジョブリソースを使用して、ライブコンテンツストリームから Live-to-VOD (ビデオオンデマンド) アセットを抽出します。はアセット MediaPackage を作成し、Amazon S3 バケットに保存します。の VOD 機能を使用して MediaPackage 、アセットをエンドユーザーに配信できます。

### 入力冗長

入力冗長は、MediaPackage でのライブワークフローでのみ使用できます。

MediaPackage は、各チャンネルに 2 つの入力 URLs を作成するため、同じチャンネルに 2 つの同一のストリームを送信することで入力冗長を作成できます。入力冗長の仕組みについては、「[ライブ入力冗長の AWS Elemental MediaPackage 処理の流れ](#)」を参照してください。

### 字幕

MediaPackage は、入力 WebVTT テキストベースの字幕をサポートしています。MediaPackage は、エンドポイントで使用されるパッケージに基づいて、字幕を適切な形式に変換します。

- HLS および CMAF の場合: WebVTT をパススルーする
- DASH の場合: サブタイトルを EBU-TT に変換する
- Microsoft Smooth Streaming の場合: サブタイトルを DFXP に変換する

#### Important

MediaPackage は、HLS ソースから作成された VOD アセットに対してのみ、HLS、CMAF、DASH マニフェストのアクセシビリティシグナリングをサポートします。HLS ソースプレイリストの EXT-X-MEDIA 行には、`public.accessibility.describes-music-and-sound` または `public.accessibility.transcribes-spoken-dialog` の特性属性が含まれている必要があります。

### タイムシフト表示

タイムシフト表示は、MediaPackage でのライブワークフローでのみ使用できます。

MediaPackage では、現在の時刻より前の時刻にストリームを再生できます。スタートオーバー、キャッチアップ TV、時間遅延のすべてがサポートされています。タイムシフト機能の設定の詳細については、「[AWS Elemental MediaPackage のタイムシフト表示のリファレンス](#)」を参照してください。

## 動画

MediaPackage は、入力 H.264 ビデオコーデックをサポートし、出力ストリームに渡します。の CMAF エンドポイントは、該当する再生デバイスに対する Apple 仕様に従って、H.265/HEVC および HDR-10 MediaPackage もサポートしています。

### Important

MediaPackage では、エンコーダーからのストリーム設定に少なくとも 1 つのビデオトラックが存在する必要があります。このサービスは音声のみの取り込みをサポートしていません。

## ホワイトリスト

ホワイトリストは、MediaPackage でのライブワークフローでのみ使用できます。

MediaPackage は、エンドポイントへのネットワークアクセスの制限をサポートしています。この機能を利用するには、許可されているエンドポイントの IP アドレスを入力する必要があります。ホワイトリスト情報の詳細については、「[アクセスコントロールの設定フィールド](#)」を参照してください。

## 関連サービス

- Amazon CloudFront は、データと動画を視聴者に安全に配信するグローバルコンテンツ配信ネットワーク (CDN) サービスです。CloudFront では、最大限のパフォーマンスでコンテンツを配信します。詳細については、「[Amazon CloudFront](#)」を参照してください。
- Amazon CloudWatch は、AWS クラウドリソースとで実行するアプリケーションのモニタリングサービスです。AWS を使用して CloudWatch、コンテンツの入力および出力リクエスト数などのメトリクスを追跡します。詳細については、「[Amazon CloudWatch](#)」を参照してください。
- AWS Elemental MediaLive (MediaLive) は、ブロードキャストテレビやマルチスクリーンデバイス向けに高品質のライブビデオストリームをエンコードするライブビデオ処理サービスです。MediaLive を使用してコンテンツストリームをエンコードし、パッケージ化 MediaPackage



のために送信します。エンコーダー (など MediaLive) がと連携する方法の詳細については MediaPackage、 「」を参照してください [MediaPackage の仕組み](#)。

- AWS Identity and Access Management (IAM) は、AWS リソースへのユーザーアクセスをセキュアに管理するウェブサービスです。IAM を使用して、どのユーザーが AWS リソースを使用できるかを制御し (認証)、さらに、どのリソースをユーザーがどのように使用できるかを制御します (権限付与)。詳細については、「[設定](#)」を参照してください。
- AWS Elemental MediaTailor (MediaTailor) は、AWS クラウドで実行されるスケーラブルな広告挿入サービスです。を使用して MediaTailor、ターゲットを絞った広告を視聴者に配信します。詳細については、「[AWS Elemental MediaTailor](#)」を参照してください。
- Amazon Simple Storage Service (Amazon S3) は、ストレージサービスです。Amazon S3 からビデオオンデマンド (VOD) アセットをプルしたり、選択したバケットに Live-to-VOD アセットを保存できます。詳細については、「[MediaPackage での VOD コンテンツの配信開始](#)」および「[MediaPackage での live-to-VOD コンテンツ配信の開始](#)」を参照してください。

## アクセス MediaPackage

次のいずれか MediaPackage の方法でにアクセスできます。

- AWS マネジメントコンソール - このガイドの手順では、AWS マネジメントコンソールを使用してのタスクを実行する方法について説明します MediaPackage。

```
https://console.aws.amazon.com/mediapackage/
```

- AWS Command Line Interface - 詳細については、[AWS Command Line Interface ユーザーガイド](#)を参照してください。

```
aws mediapackage
```

- MediaPackage API - API アクションの詳細と API リクエストの作成方法については、「API [AWS Elemental MediaConnect リファレンス](#)」を参照してください。

```
https://mediapackage.region.amazonaws.com
```

- AWS SDKs - が SDK AWSを提供するプログラミング言語を使用している場合は、SDK を使用してにアクセスできます MediaPackage。SDK では、認証を簡素化し、開発環境と容易に統合して、MediaPackage のコマンドに簡単にアクセスできます。詳細については、「[Amazon ウェブサービスのツール](#)」を参照してください。



- AWS Tools for Windows PowerShell - 詳細については、[AWS Tools for Windows PowerShell 「ユーザーガイド」](#) を参照してください。

## の料金 MediaPackage

他の AWS 製品と同様、MediaPackage を使用するための契約や最低契約金は必要ありません。アカウントで使用した AWS リソースに対してのみ、料金が発生します。料金は pay-as-you-go であり、次の内容で構成されます。

- 受信したコンテンツの 1 GB あたりの料金
- からストリーミングされたコンテンツに対する GB あたりの料金 MediaPackage

この 1 GB あたりの料金は、コンテンツ配信ネットワークからキャッシュして使用したコンテンツに対しては発生しません。

料金の詳細については、「[MediaPackage の料金表](#)」を参照してください。

## のリージョン MediaPackage

アプリケーションのレイテンシーを減らすために、はリクエストのリージョンエンドポイント MediaPackage を提供します。MediaPackage が利用可能な AWS リージョンのリストを表示するには、[MediaPackage 「リージョン」](#) を参照してください。

# セットアップ MediaPackage

AWS Elemental MediaPackage (MediaPackage) を使い始める前に、(AWS アカウントをまだお持ちでない場合) サインアップして、アクセスを許可する IAM ユーザーとロールを作成する必要があります。AWS MediaPackage には、自分自身の IAM ロールを作成することが含まれます。暗号化を使用してコンテンツを保護する場合は、暗号化キーを保存し AWS Secrets Manager、Secrets Manager MediaPackage アカウントからキーを取得する権限を与える必要もあります。

このセクションでは、MediaPackage アクセスするユーザーとロールを設定するために必要な手順を順を追って説明します。の ID とアクセス管理の背景と追加情報については MediaPackage、を参照してください [the section called “Identity and Access Management”](#)。

## トピック

- [へのサインアップ AWS](#)
- [ポリシーと管理者以外のロールの作成](#)
- [他の AWS サービスへのアクセスを AWS Elemental MediaPackage に許可する](#)
- [\(オプション\) 暗号化の設定](#)
- [\(オプション\) をインストールします。AWS CLI](#)

## へのサインアップ AWS

### トピック

- [にサインアップ AWS アカウント](#)
- [管理者権限を持つユーザーを作成します。](#)

## にサインアップ AWS アカウント

をお持ちでない場合は AWS アカウント、次の手順を実行して作成してください。

にサインアップするには AWS アカウント

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

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

にサインアップすると AWS アカウント、AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティ上のベストプラクティスとして、管理アクセス権をユーザーに割り当て、[ルートユーザーアクセスを必要とするタスクの実行には root ユーザーのみを使用してください](#)。

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

## 管理者権限を持つユーザーを作成します。

にサインアップしたら AWS アカウント、日常のタスクに root ユーザーを使用しないように AWS IAM Identity Center、管理ユーザーを保護し、有効にしてから作成してください。AWS アカウントのルートユーザー

セキュリティを確保してください。AWS アカウントのルートユーザー

1. [Root user] を選択し、AWS アカウント メールアドレスを入力して、[AWS Management Console](#) アカウント所有者としてログインします。次のページでパスワードを入力します。

ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドの「[ルートユーザーとしてサインインする](#)」を参照してください。

2. ルートユーザーの多要素認証 (MFA) を有効にします。

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

管理者権限を持つユーザーを作成します。

1. IAM アイデンティティセンターを有効にします。

手順については、「AWS IAM Identity Center ユーザーガイド」の「[AWS IAM Identity Centerの有効化](#)」を参照してください。

2. IAM Identity Center で、ユーザーに管理アクセスを付与します。

IAM アイデンティティセンターディレクトリ をアイデンティティソースとして使用するチュートリアルについては、『ユーザーガイド』の「[IAM アイデンティティセンターディレクトリデフォルトでのユーザーアクセスの設定](#)」を参照してください。AWS IAM Identity Center

管理者権限を持つユーザーとしてサインインします。

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

IAM Identity Center [ユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドの「AWS アクセスポータルへのサインイン」](#)を参照してください。

追加のユーザーにアクセス権を割り当てます。

1. IAM Identity Center で、最小権限の権限を適用するというベストプラクティスに従った権限セットを作成します。

手順については、『ユーザーガイド』の「[権限セットの作成](#)」を参照してください。AWS IAM Identity Center

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

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

## ポリシーと管理者以外のロールの作成

デフォルトでは、MediaPackageユーザーとロールにはリソースを作成または変更する権限がありません。また、AWS Management Console、AWS Command Line Interface (AWS CLI)、AWS API を使用してタスクを実行することもできません。IAM 管理者は、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。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、『IAM ユーザーガイド』の「[IAM ポリシーの作成](#)」を参照してください。

各リソースタイプの ARN の形式など MediaPackage、で定義されるアクションとリソースタイプの詳細については、『サービス認証リファレンス』の「[アクション、リソース、および条件キー](#)」を参照してください。AWS Elemental MediaPackage

このセクションでは、MediaPackage ユーザーがリソースを作成または変更できるように、ポリシーを作成して非管理者ロールを作成する方法について説明します。このセクションでは、ユーザーがそのロールを引き受け、安全で一時的な認証情報を付与する方法についても説明します。

## トピック

- [\(オプション\) ステップ 1: Amazon の IAM ポリシーを作成する CloudFront](#)
- [\(オプション\) ステップ 2: VOD 用の IAM ポリシーを作成する MediaPackage](#)
- [ステップ 3: IAM コンソールでロールを作成する](#)
- [ステップ 4: IAM コンソールからロールを引き受けるか、AWS CLI](#)

## (オプション) ステップ 1: Amazon の IAM ポリシーを作成する CloudFront

AWS Elemental MediaPackage あなたまたはあなたのユーザーがライブコンソールから Amazon CloudFront デイストリビューションを作成する場合は、へのアクセスを許可する IAM ポリシーを作成してください。CloudFront

CloudFront with の使用について詳しくは MediaPackage、「」を参照してください。[CDN の使用](#)

JSON ポリシーエディタでポリシーを作成するには

1. AWS Management Console にサインインし、<https://console.aws.amazon.com/iam/> にある IAM コンソールを開きます。
2. 左側のナビゲーションペインで、[ポリシー] を選択します。

初めて [ポリシー] を選択する場合には、[管理ポリシーによろこそ] ページが表示されます。[今すぐ始める] を選択します。

3. ページの上部で、[ポリシーを作成] を選択します。
4. [ポリシーエディタ] セクションで、[JSON] オプションを選択します。
5. 次の JSON ポリシードキュメントを入力します。

```
{  
  "Version": "2012-10-17",
```

```
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "cloudfront:GetDistribution",
      "cloudfront:CreateDistributionWithTags",
      "cloudfront:UpdateDistribution",
      "cloudfront:CreateDistribution",
      "cloudfront:TagResource",
      "tag:GetResources"
    ],
    "Resource": "*"
  }
]
```

6. [次へ] をクリックします。

#### Note

いつでも [Visual] と [JSON] エディタオプションを切り替えることができます。ただし、[Visual] エディタで [次] に変更または選択した場合、IAM はポリシーを再構成して visual エディタに合わせて最適化することがあります。詳細については、「IAM ユーザーガイド」の「[ポリシーの再構成](#)」を参照してください。

7. [確認と作成] ページで、作成するポリシーの [ポリシー名] と [説明] (オプション) を入力します。[このポリシーで定義されているアクセス許可] を確認して、ポリシーによって付与されたアクセス許可を確認します。
8. [ポリシーの作成] をクリックして、新しいポリシーを保存します。

## (オプション) ステップ 2: VOD 用の IAM ポリシーを作成する MediaPackage

管理者またはユーザーがビデオオンデマンド (VOD) 機能を使用する場合は MediaPackage、サービスのリソースへのアクセスを許可する IAM ポリシーを作成してください。mediapackage-vod

以下のセクションでは、すべてのアクションを許可するポリシーと、読み取り専用権限を付与するポリシーを作成する方法について説明します。ワークフローに合うようにアクションを追加または削除することで、ポリシーをカスタマイズできます。

## VOD へのフルアクセスのポリシー

このポリシーでは、すべての VOD リソースに対するすべてのアクションの実行をユーザーに許可します。

JSON ポリシーエディタでポリシーを作成するには

1. AWS Management Console [にサインインし、https://console.aws.amazon.com/iam/ にある IAM コンソールを開きます。](https://console.aws.amazon.com/iam/)
2. 左側のナビゲーションペインで、[ポリシー] を選択します。

初めて [ポリシー] を選択する場合には、[管理ポリシーによるこそ] ページが表示されます。[今すぐ始める] を選択します。

3. ページの上部で、[ポリシーを作成] を選択します。
4. [ポリシーエディタ] セクションで、[JSON] オプションを選択します。
5. 次の JSON ポリシードキュメントを入力します。

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

6. [次へ] をクリックします。

### Note

いつでも [Visual] と [JSON] エディタオプションを切り替えることができます。ただし、[Visual] エディタで [次] に変更または選択した場合、IAM はポリシーを再構成して visual エディタに合わせて最適化することがあります。詳細については、「IAM ユーザーガイド」の「[ポリシーの再構成](#)」を参照してください。

7. [確認と作成] ページで、作成するポリシーの [ポリシー名] と [説明] (オプション) を入力します。 [このポリシーで定義されているアクセス許可] を確認して、ポリシーによって付与されたアクセス許可を確認します。
8. [ポリシーの作成] をクリックして、新しいポリシーを保存します。

## 読み取り専用の VOD へのアクセスのポリシー

このポリシーでは、すべての VOD リソースの表示をユーザーに許可します。

JSON ポリシーエディタでポリシーを作成するには

1. AWS Management Console [にサインインし、https://console.aws.amazon.com/iam/ の IAM コンソールを開きます。](https://console.aws.amazon.com/iam/)
2. 左側のナビゲーションペインで、[ポリシー] を選択します。

初めて [ポリシー] を選択する場合には、[管理ポリシーによるこそ] ページが表示されます。[今すぐ始める] を選択します。

3. ページの上部で、[ポリシーを作成] を選択します。
4. [ポリシーエディタ] セクションで、[JSON] オプションを選択します。
5. 次の JSON ポリシードキュメントを入力します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mediapackage-vod:List*",
        "mediapackage-vod:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

6. [次へ] をクリックします。



**Note**

いつでも [Visual] と [JSON] エディタオプションを切り替えることができます。ただし、[Visual] エディタで [次] に変更または選択した場合、IAM はポリシーを再構成して visual エディタに合わせて最適化することがあります。詳細については、「IAM ユーザーガイド」の「[ポリシーの再構成](#)」を参照してください。

7. [確認と作成] ページで、作成するポリシーの [ポリシー名] と [説明] (オプション) を入力します。[このポリシーで定義されているアクセス許可] を確認して、ポリシーによって付与されたアクセス許可を確認します。
8. [ポリシーの作成] をクリックして、新しいポリシーを保存します。

## ステップ 3: IAM コンソールでロールを作成する

作成するポリシーごとに IAM コンソールでロールを作成します。これにより、各ユーザーに個別のポリシーをアタッチするのではなく、ユーザーがロールを引き受けることができます。

IAM コンソールでロールを作成するには

1. AWS Management Console [にサインインし、https://console.aws.amazon.com/iam/ の IAM コンソールを開きます。](https://console.aws.amazon.com/iam/)
2. IAM コンソールのナビゲーションペインで、[ロール]、[ロールを作成] を選択します。
3. [信頼されたエンティティを選択] で、[AWS アカウント] を選択します。
4. 「AWS アカウント」で、このロールを引き受けるユーザーのアカウントを選択します。
  - このロールにサードパーティがアクセスする場合は、[Require external ID] を選択するのがベストプラクティスです。外部 ID の詳細については、IAM ユーザーガイドの[第三者によるアクセスのための外部 ID の使用](#)を参照してください。
  - 多要素認証 (MFA) を要求するのがベストプラクティスです。[MFA が必要] の横にあるチェックボックスをオンにします。MFA の詳細については、IAM ユーザーガイドの[多要素認証 \(MFA\)](#)を参照してください。
5. [次へ] をクリックします。
6. [権限ポリシー] で、MediaPackage 適切な権限レベルのポリシーを検索して追加します。
  - ライブ機能へのアクセスには、次のオプションのいずれかを選択します。

- AWSElementalMediaPackageFullAccessを使用して、内のすべてのライブラリソースに対してユーザーがすべてのアクションを実行できるようにします MediaPackage。
  - AWSElementalMediaPackageReadOnlyを使用して、内のすべてのライブラリソースに対する読み取り専用権限をユーザーに付与します。 MediaPackage
  - ビデオオンデマンド (VOD) 機能にアクセスするには、[「\(オプション\) ステップ 2: VOD 用の IAM ポリシーを作成する MediaPackage」](#) で作成したポリシーを使用します。
7. MediaPackage コンソールがユーザーに代わって Amazon CloudWatch に電話をかけることを許可するポリシーを追加します。これらのポリシーがないと、ユーザーが使用できるのはサービスの API のみとなり、コンソールは使用できません。以下のオプションのいずれかを選択します。
- ReadOnlyAccessを使用して、 MediaPackage AWS アカウントのすべてのサービスとの通信を許可し CloudWatch、ユーザーには読み取り専用アクセス権を付与します。
  - CloudWatchReadOnlyAccess、CloudWatchEventsReadOnlyAccess、MediaPackage を使用してとの通信を許可し CloudWatch、ユーザーの読み取り専用アクセスを制限します。CloudWatchLogsReadOnlyAccess CloudWatch
8. (オプション) MediaPackage このユーザーがコンソールから Amazon CloudFront ディストリビューションを作成する場合は、[\(オプション\) ステップ 1: Amazon の IAM ポリシーを作成する CloudFront](#)で作成したポリシーをアタッチします。
9. (オプション) [アクセス許可の境界](#)を設定します。このアドバンスド機能は、サービスロールで使用できますが、サービスにリンクされたロールではありません。
1. [Permissions boundary] (アクセス許可の境界) セクションを展開し、[Use a permissions boundary to control the maximum role permissions] (アクセス許可の境界を使用して、ロールのアクセス許可の上限を設定する) を選択します。IAM には、AWS アカウント内の管理ポリシーとカスタマー管理ポリシーのリストが含まれます。
  2. アクセス許可の境界に使用するポリシーを選択するか、[ポリシーを作成] を選択して新しいブラウザタブを開き、新しいポリシーをゼロから作成します。詳細については、『IAM ユーザーガイド』の「[IAM ポリシーの作成](#)」を参照してください。
  3. ポリシーを作成したら、そのタブを閉じて元のタブに戻り、アクセス許可の境界として使用するポリシーを選択します。
10. このグループに正しいポリシーが追加されていることを確認し、[次へ] を選択します。
11. 可能な場合は、このロールの目的を識別するのに役立つロール名またはロール名サフィックスを入力します。ロール名は AWS アカウントアカウント内で一意である必要があります。大文字と小文字は区別されません。例えば、**PRODRROLE** と **prodrole** というロール名を両方作成するこ

とはできません。多くのエンティティによりロールが参照されるため、作成後にロール名を変更することはできません。

12. (オプション) [Description (説明)] には、新しいロールの説明を入力します。
13. [Step 1: Select trusted entities] (ステップ 1: 信頼済みエンティティの選択) または [Step 2: Select permissions] (ステップ 2: 権限の選択) のセクションで [Edit] (編集) を選択し、ロールのユースケースと権限を変更します。
14. (オプション) タグをキーバリューペアとしてアタッチして、メタデータをユーザーに追加します。IAM でのタグの使用に関する詳細については、「IAM ユーザーガイド」の「[IAM リソースにタグを付ける](#)」を参照してください。
15. ロール情報を確認し、ロールの作成 を選択します。

## ステップ 4: IAM コンソールからロールを引き受けるか、AWS CLI

ロールを引き受けるためのアクセス許可をユーザーに付与する方法と、ユーザーが IAM コンソールまたは AWS CLI からそのロールに切り替える方法については、以下のリソースをご覧ください。

- ロールを切り替えるユーザー許可の付与に関する詳細については、IAM ユーザーガイドの「[ロールを切り替えるアクセス許可をユーザーに付与する](#)」を参照してください。
- ロールの切り替え (コンソール) に関する詳細については、IAM ユーザーガイドの「[ロールの切り替え \(コンソール\)](#)」を参照してください。
- ロールの切り替え (AWS CLI) に関する詳細については、IAM ユーザーガイドの「[IAM ロール \(AWS CLI\) の切り替え](#)」を参照してください。

## 他の AWS サービスへのアクセスを AWS Elemental MediaPackage に許可する

一部の機能では、MediaPackage に対して他の AWS サービス (Amazon S3、AWS Secrets Manager (Secrets Manager) など) へのアクセスを許可する必要があります。このアクセスを許可するには、適切なアクセス許可を持つ IAM ロールとポリシーを作成します。次の手順では、MediaPackage の機能のロールとポリシーを作成する方法について説明します。

### トピック

- [ステップ 1: ポリシーの作成](#)
- [ステップ 2: ロールの作成](#)

- [ステップ 3: 信頼関係の変更](#)

## ステップ 1: ポリシーの作成

IAM ポリシーは、他のサービスにアクセスするために AWS Elemental MediaPackage (MediaPackage) が必要とするアクセス許可を定義します。

- ビデオオンデマンド (VOD) ワークフローの場合、Amazon S3 バケットからの読み取り、課金方法の確認、コンテンツの取得を MediaPackage に許可するポリシーを作成します。請求方法については、MediaPackage で、バケットがリクエストに対する支払いをリクエストに請求しないことを確認する必要があります。バケットで requestPayment が有効になっている場合、MediaPackage でそのバケットからコンテンツを取り込むことができません。
- Live-to-VOD ワークフローの場合、Amazon S3 バケットからの読み取りおよびバケットへの Live-to-VOD アセットの保存を MediaPackage に許可するポリシーを作成します。
- コンテンツ配信ネットワーク (CDN) 認証については、Secrets Manager のシークレットからの読み取りを MediaPackage に許可するポリシーを作成します。

次のセクションでは、これらのポリシーの作成方法について説明します。

### トピック

- [VOD ワークフローでの Amazon S3 へのアクセス](#)
- [Live-to-VOD ワークフローのポリシー](#)
- [CDN 認証での Secrets Manager へのアクセス](#)

## VOD ワークフローでの Amazon S3 へのアクセス

MediaPackage を使用して Amazon S3 バケットから VOD アセットを取り込み、そのアセットをパッケージ化して配信する場合、Amazon S3 で次の操作の実行を許可するポリシーが必要です。

- GetObject - MediaPackage でバケットから VOD アセットを取得できます。
- GetBucketLocation - MediaPackage でバケットのリージョンを取得できます。バケットは MediaPackage VOD のリソースと同じリージョンにある必要があります。
- GetBucketRequestPayment - MediaPackage で支払いリクエストの情報を取得できます。MediaPackage では、バケットでコンテンツリクエストの支払いをリクエストに求めないことを確認するためにこの情報を使用します。

Live-to-VOD アセットの収集にも MediaPackage を使用する場合は、ポリシーに PutObject アクションを追加します。Live-to-VOD ワークフローに必要なポリシーの詳細については、「[Live-to-VOD ワークフローのポリシー](#)」を参照してください。

JSON ポリシーエディタでポリシーを作成するには

1. AWS Management Console にサインインして、IAM コンソール (<https://console.aws.amazon.com/iam/>) を開きます。
2. 左側のナビゲーションペインで、[ポリシー] を選択します。

初めて [ポリシー] を選択する場合には、[管理ポリシーによるこそ] ページが表示されます。[今すぐ始める] を選択します。

3. ページの上部で、[ポリシーを作成] を選択します。
4. [ポリシーエディタ] セクションで、[JSON] オプションを選択します。
5. 次の JSON ポリシードキュメントを入力します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:GetBucketRequestPayment",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::bucket_name/*",
        "arn:aws:s3:::bucket_name"
      ],
      "Effect": "Allow"
    }
  ]
}
```

6. [次へ] をクリックします。

**Note**

いつでも [Visual] と [JSON] エディタオプションを切り替えることができます。ただし、[Visual] エディタで [次] に変更または選択した場合、IAM はポリシーを再構成して visual エディタに合わせて最適化することがあります。詳細については、『IAM ユーザーガイド』の「[ポリシーの再構成](#)」を参照してください。

7. [確認と作成] ページで、作成するポリシーの [ポリシー名] と [説明] (オプション) を入力します。[このポリシーで定義されているアクセス許可] を確認して、ポリシーによって付与されたアクセス許可を確認します。
8. [ポリシーの作成] をクリックして、新しいポリシーを保存します。

## Live-to-VOD ワークフローのポリシー

MediaPackage を使用してライブストリームから Live-to-VOD アセットを収集する場合、Amazon S3 で次の実行を許可するポリシーが必要です。

- PutObject: MediaPackage で VOD アセットをバケットに保存できます。
- GetBucketLocation: MediaPackage でバケットのリージョンを取得できます。バケットは MediaPackage VOD のリソースと同じ AWS リージョンにある必要があります。

VOD アセットの配信にも MediaPackage を使用する場合、ポリシーに GetObject および GetBucketRequestPayment アクションを追加します。VOD ワークフローに必要なポリシーの詳細については、「[VOD ワークフローでの Amazon S3 へのアクセス](#)」を参照してください。

JSON ポリシーエディタでポリシーを作成するには

1. AWS Management Console にサインインして、IAM コンソール (<https://console.aws.amazon.com/iam/>) を開きます。
2. 左側のナビゲーションペインで、[ポリシー] を選択します。  
  
初めて [ポリシー] を選択する場合には、[管理ポリシーによるこそ] ページが表示されます。[今すぐ始める] を選択します。
3. ページの上部で、[ポリシーを作成] を選択します。
4. [ポリシーエディタ] セクションで、[JSON] オプションを選択します。
5. 次の JSON ポリシードキュメントを入力します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:PutObject",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::bucket_name/*",
        "arn:aws:s3:::bucket_name"
      ],
      "Effect": "Allow"
    }
  ]
}
```

6. [次へ] をクリックします。

#### Note

いつでも [Visual] と [JSON] エディタオプションを切り替えることができます。ただし、[Visual] エディタで [次] に変更または選択した場合、IAM はポリシーを再構成して visual エディタに合わせて最適化することがあります。詳細については、『IAM ユーザーガイド』の「[ポリシーの再構成](#)」を参照してください。

7. [確認と作成] ページで、作成するポリシーの [ポリシー名] と [説明] (オプション) を入力します。[このポリシーで定義されているアクセス許可] を確認して、ポリシーによって付与されたアクセス許可を確認します。
8. [ポリシーの作成] をクリックして、新しいポリシーを保存します。

## CDN 認証での Secrets Manager へのアクセス

コンテンツ配信ネットワーク (CDN) 認証ヘッダーを使用して MediaPackage のエンドポイントへのアクセスを制限する場合、Secrets Manager で次の実行を許可するポリシーが必要です。

- GetSecretValue - MediaPackage でシークレットのバージョンから暗号化された認証コードを取得できます。



- DescribeSecret - MediaPackage で暗号化されたフィールドを除いてシークレットの詳細を取得できます。
- ListSecrets - MediaPackage で AWS アカウント内のシークレットのリストを取得できます。
- ListSecretVersionIds: MediaPackage で、指定したシークレットに添付されているすべてのバージョンを取得できます。

#### Note

Secrets Manager に保存しているシークレットごとに個別のポリシーは必要ありません。次の手順で説明するようなポリシーを作成すると、MediaPackage でこのリージョンのアカウント内のすべてのシークレットにアクセスできます。

JSON ポリシーエディタを使用してポリシーを作成するには

1. AWS Management Console にサインインして、IAM コンソール (<https://console.aws.amazon.com/iam/>) を開きます。
2. 左側のナビゲーション列で、[ポリシー] を選択します。

[Policies] (ポリシー) を初めて選択する場合は、[Welcome to Managed Policies] (マネージドポリシーによる) ページが表示されます。[Get Started] (今すぐ始める) を選択します。

3. ページの上部で、[ポリシーの作成] を選択します。
4. [JSON] タブを選択します。
5. 次の JSON ポリシードキュメントを入力し、*region*、*account-id*、*secret-name*、*role-name* をお客様自身の情報で置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource": [
```



```
    "arn:aws:secretsmanager:region:account-id:secret:secret-name"
  ],
},
{
  "Effect": "Allow",
  "Action": [
    "iam:GetRole",
    "iam:PassRole"
  ],
  "Resource": "arn:aws:iam::account-id:role/role-name"
}
]
```

6. [ポリシーの確認] を選択します。

#### Note

いつでも [Visual editor] (ビジュアルエディタ) タブと [JSON] タブを切り替えることができます。ただし、[Visual editor] (ビジュアルエディタ) タブで [Review policy] (ポリシーの確認) を変更または選択した場合、IAM はポリシーを再構成してビジュアルエディタに合わせて最適化することがあります。詳細については、IAM ユーザーガイドの「[ポリシーの再構成](#)」を参照してください。

7. [ポリシーの確認] ページに作成するポリシーの [名前] と [説明] を入力します。ポリシーの [Summary] (概要) を参照して、ポリシーによって付与された許可を確認します。次に、[Create policy] (ポリシーの作成) を選択して作業を保存します。

## ステップ 2: ロールの作成

IAM [ロール](#) は、特定の許可があり、アカウントで作成できるもう 1 つの IAM アイデンティティです。IAM ロールは、ID が AWS で実行できることとできないことを決定する許可ポリシーを持つ AWS ID であるという点で IAM ユーザーと似ています。ただし、ユーザーは 1 人の特定の人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。また、ロールには標準の長期認証情報 (パスワードやアクセスキーなど) も関連付けられません。代わりに、ロールを引き受けると、ロールセッション用の一時的なセキュリティ認証情報が提供されます。Amazon S3 からソースコンテンツを取り込むときに、AWS Elemental MediaPackage が引き受けるロールを作成します。

ロールを作成する際、MediaPackage は選択できないため、ロールを引き受けることができる信頼されたエンティティとして Amazon Elastic Compute Cloud (Amazon EC2) を選択します。[ステップ 3: 信頼関係の変更](#) で、信頼されたエンティティを MediaPackage に変更します。

EC2 の信頼されたエンティティ用にサービスロールを作成するには (IAM コンソール)

1. AWS Management Console にサインインして、IAM コンソール (<https://console.aws.amazon.com/iam/>) を開きます。
2. IAM コンソールのナビゲーションペインで、[ロール]、[ロールを作成] を選択します。
3. 信頼できるエンティティタイプで、AWS のサービス を選択します。
4. [Service or use case (ユースケースの選択)] で [EC2 trusted entity (EC2 の信頼されたエンティティ)] を選択し、[EC2] ユースケースを選択します。
5. [次へ] をクリックします。
6. [Attach permissions policies] (アクセス許可ポリシーのアタッチ) ページで、[ステップ 1: ポリシーの作成](#) で作成したポリシーを検索し、選択します。[Next: Tags] (次へ: タグ)、[Next: Review] (次へ: 確認) の順に選択します。
7. (オプション) [アクセス許可の境界](#)を設定します。このアドバンスド機能は、サービスロールで使用できますが、サービスにリンクされたロールではありません。
  - a. [Set permissions boundary (アクセス許可の境界の設定)] セクションを開き、[Use a permissions boundary to control the maximum role permissions (アクセス許可の境界を使用してロールのアクセス許可の上限を設定する)] を選択します。

IAM には、あなたのアカウント内の AWS 管理ポリシーとカスタマー管理ポリシーのリストがあります。
  - b. アクセス許可の境界として使用するポリシーを選択します。
8. [次へ] をクリックします。
9. ロールの目的を識別するのに役立つロール名またはロール名サフィックスを入力します。

**⚠ Important**

ロールに名前を付ける際は、以下の点に注意してください。

- ロール名は AWS アカウント 内で一意でなければなりません。大文字と小文字は区別されません。

例えば、**PRODROLE** と **prodrole** というロール名を両方作成しないでください。ロール名がポリシーで、または ARN の一部として使用される場合、大文字と小文字が区別されますが、サインイン中など、コンソールにロール名が表示される場合は、大文字と小文字は区別されません。

- 他のエンティティがロールを参照する可能性があるため、作成後にロール名を編集することはできません。

10. (オプション) [Description (説明)] には、ロールの説明を入力します。
11. (オプション) [Step 1: Select trusted entities] (ステップ 1: 信頼済みエンティティの選択) または [Step 2: Add permissions] (ステップ 2: 権限の追加) のセクションで [Edit] (編集) を選択し、ロールのユースケースと権限を変更します。
12. (オプション) ロールの特定、整理、検索をサポートするため、キーと値のペアでタグを追加します。IAM でのタグの使用に関する詳細については、「IAM ユーザーガイド」の「[IAM リソースにタグを付ける](#)」を参照してください。
13. ロールを確認したら、[Create role] (ロールを作成) を選択します。

## ステップ 3: 信頼関係の変更

信頼関係は、[the section called “ステップ 2: ロールの作成”](#) で作成したロールをどのエンティティが引き受けることができるかを定義します。ロールを作成して信頼関係を確立する際に、信頼されたエンティティとして Amazon EC2 を選択しました。ロールを変更して、AWS アカウントと AWS Elemental MediaPackage の間に信頼関係を設定します。

MediaPackage に対する信頼関係を変更するには

1. [ステップ 2: ロールの作成](#) で作成したロールにアクセスします。

まだロールを表示していない場合は、IAM コンソールのナビゲーションペインで [Roles] (ロール) を選択します。作成したロールを検索し、選択します。

2. そのロールの [Summary (概要)] ページで、[Trust relationship (信頼関係)] を選択します。
3. [信頼関係の編集] を選択します。
4. [Edit Trust Relationship (信頼関係の編集)] ページの [Policy Document (ポリシードキュメント)] で、`ec2.amazonaws.com` を `mediapackage.amazonaws.com` に変更します。

ポリシードキュメントは次のようになります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "mediapackage.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

5. 信頼ポリシーの更新 を選択します。
6. [Summary] (概要) ページで、[Role ARN] (ロール ARN) の値をメモします。ビデオオンデマンド (VOD) ワークフローのソースコンテンツを取得するとき、この ARN を使用します。ARN は次のようになります。

```
arn:aws:iam::111122223333:role/role-name
```

この例では、**111122223333** が AWS のアカウント番号です。

## (オプション) 暗号化の設定

コンテンツ暗号化とデジタル著作権管理 (DRM) により、コンテンツを不正使用から保護します。AWS Elemental MediaPackage [AWS セキュア・パッケージャーおよびエンコーダー・キー・エクスチェンジ \(SPEKE\) API](#) を使用して、DRM プロバイダーによるコンテンツの暗号化と復号化を容易にします。DRM プロバイダーは SPEKE を使用して SPEKE API を通じて暗号化キーを提供します。MediaPackage 同時に DRM プロバイダーは、サポートしているメディアプレイヤー用に復号化のためのライセンスも提供します。クラウドで実行されているサービスや機能での SPEKE の使用については、Secure Packager and Encoder Key Exchange API Specification guide の「[AWS cloud-based architecture](#)」を参照してください。

コンテンツを暗号化するには、DRM ソリューションプロバイダーが必要で、暗号化を使用するように設定する必要があります。詳細については、「[the section called “コンテンツの暗号化と DRM”](#)」を参照してください。

## (オプション) をインストールします。 AWS CLI

AWS CLI with を使用するには AWS Elemental MediaPackage、AWS CLI 最新バージョンをインストールします。AWS CLI のインストールや最新バージョンへのアップグレードについては、『AWS Command Line Interface ユーザーガイド』の「[AWS Command Line Interfaceのインストール](#)」を参照してください。

# AWS Elemental MediaPackage の開始方法

次のセクションでは、AWS Elemental MediaPackage を使用してコンテンツをすばやく送受信する方法について説明します。

## トピック

- [AWS Elemental MediaPackage でのライブコンテンツ配信の開始](#)
- [MediaPackage での live-to-VOD コンテンツ配信の開始](#)
- [MediaPackage での VOD コンテンツの配信開始](#)

## AWS Elemental MediaPackage でのライブコンテンツ配信の開始

この入門チュートリアルでは、AWS Elemental MediaPackage (MediaPackage) コンソールを使用して、ライブ動画のストリーミングのためにチャンネルとエンドポイントを作成する方法を説明します。

## トピック

- [前提条件](#)
- [ステップ 1: MediaPackage にアクセスする](#)
- [ステップ 2: チャンネルを作成する](#)
- [ステップ 3: エンドポイントを作成する](#)
- [\(オプション\) ステップ 4: MediaPackage のアクティビティをモニタリングする](#)
- [ステップ 5: クリーンアップ](#)

## 前提条件

MediaPackage を使用するには、事前に AWS アカウントが必要です。また、MediaPackage コンポーネントにアクセスして表示や編集を行うための適切なアクセス許可が必要です。システム管理者が [設定](#) の手順を完了したことを確認してから、このチュートリアルに戻ってください。

サポートされているライブ入力とコーデックについては、「[ライブでサポートされるコーデックおよび入力タイプ](#)」を参照してください。。

## ステップ 1: MediaPackage にアクセスする

IAM 認証情報を使用して、MediaPackage コンソールにサインインします。

<https://console.aws.amazon.com/mediapackage/>

## ステップ 2: チャンネルを作成する

チャンネルは MediaPackage の最初のコンポーネントです。チャンネルは、AWS Elemental MediaLive などのエンコーダーからのライブコンテンツを受け取る、MediaPackage の入力に対応します。

MediaPackage に対しては、ユーザーが個人データを提供する必要はありません。お客様によるお客様データの供給が予想されるチャンネルにフィールドはありません。

### チャンネルを作成する

1. MediaPackage の [Channels] (チャンネル) ページで、[Create channel] (チャンネルの作成) をクリックします。
2. [ID] に、チャンネルを説明する名前として **channelHLS1** などと入力します。ID は、チャンネルのプライマリ識別子であり、AWS リージョン 内のアカウント別に一意である必要があります。使用できるのは、文字、数字、下線 (\_)、ダッシュ (-) のみです。ID にスペースを使用することはできません。
3. 残りのフィールドはデフォルトのままにして、[作成] を選択します。

MediaPackage が、新しいチャンネルの詳細ページを表示します。

4. チャンネルの詳細ページで、[URL]、[ユーザー名]、[パスワード] の値をメモします。入力冗長を使用している場合、両方の入力 URL でこの情報が必要です。チャンネルに 1 つのストリームのみを送信する場合は、いずれかの入力 URL の情報をメモします。

WebDAV ユーザー名とパスワードは、チャンネルの作成時に MediaPackage により安全に生成されます。これらの認証情報を変更する必要がある場合は、「[入力 URL での認証情報の更新](#)」を参照してください。

以上のフィールドの情報をアップストリームエンコーダーの担当者に渡します。エンコーダーのストリーム設定で、この担当者は入力 URL として送信先を入力し、チャンネルのユーザー名およびパスワードとして WebDAV の認証情報を入力する必要があります。アップストリームエンコーダーは、ダイジェスト認証を使用して、HTTPS 経由で WebDAV を MediaPackage にプッシュし、その際、これらの認証情報を含める必要があります。入力冗長を使用している場合は、このチャンネルへの各入力ストリームのエンコーダ設定を同じにする必要があります。入力冗長のソースストリームの設定の詳細については、「[ライブ入力冗長の AWS Elemental MediaPackage 処理の流れ](#)」を参照してください。

## ステップ 3: エンドポイントを作成する

エンドポイントは、チャンネルにアタッチされ、ライブコンテンツの出力を表します。単一のチャンネルに複数のエンドポイントに関連付けることができます。各エンドポイントは、プレーヤーとダウンロードストリーム CDN (Amazon CloudFront など) に対して、再生するコンテンツへのアクセス権を付与します。

MediaPackage に対しては、ユーザーが個人データを提供する必要はありません。エンドポイントには、お客様自身によるお客様データの供給が予想されるフィールドはありません。

エンドポイントを作成するには

1. [Channels] (チャンネル) ページで、エンドポイントに関連付けるチャンネルを選択します。
2. チャンネルの詳細ページの [オリジンエンドポイント] で、[エンドポイントの管理] を選択します。
3. [ID] に、エンドポイントを説明する名前として **HLSendpoint1** などと入力します。ID は、エンドポイントのプライマリ識別子であり、AWS リージョン 内のアカウントに対して一意である必要があります。使用できるのは、文字、数字、下線 (  )、ダッシュ (-) のみです。ID にスペースを使用することはできません。
4. 残りのフィールドはデフォルトのままにして、[Save (保存)] を選択します。

MediaPackage に、先に作成したエンドポイントを含む、チャンネルの詳細ページが表示されます。

5. チャンネルの詳細ページで、エンドポイントの [URL] フィールドの値をメモします。この情報をダウンロードストリームデバイス (CDN またはプレーヤー) の担当者に渡します。この担当者は、ダウンロードストリームデバイスでエンドポイントの URL として、リクエスト送信先を入力する必要があります。

## (オプション) ステップ 4: MediaPackage のアクティビティをモニタリングする

Amazon CloudWatch を使用して、MediaPackage によるアクティビティ (MediaPackage が受信/送信したバイト数、応答時間、リクエスト数など) を追跡します。メトリクスはまずサービスの名前空間ごとにグループ化され、次に各名前空間内のさまざまなディメンションの組み合わせごとにグループ化されます。



CloudWatch コンソールを使用してメトリクスを表示するには

1. CloudWatch コンソール (<https://console.aws.amazon.com/cloudwatch/>) を開きます。
2. ナビゲーションペインで [Metrics] (メトリクス) を選択します。
3. [All metrics] (すべてのメトリクス) で、[AWS/MediaPackage] 名前空間を選択します。
4. メトリクスディメンションを選択してメトリクスを表示します (たとえば、channel を選択してチャンネル別にメトリクスを表示します)。

MediaPackage でのメトリクスの一覧は、「[AWS Elemental MediaPackage ライブコンテンツメトリクス](#)」でご確認ください。

## ステップ 5 : クリーンアップ

不要な課金を回避するには、すべての不要なチャンネルとエンドポイントを削除してください。チャンネルを削除する前に、チャンネルのすべてのエンドポイントを削除する必要があります。

エンドポイントを削除するには

1. MediaPackage の [チャンネル] ページで、エンドポイントが関連付けられているチャンネルを選択します。
2. チャンネルの詳細ページの [オリジンエンドポイント] で、削除するオリジンエンドポイントを選択します。
3. [削除] を選択します。
4. [エンドポイントの削除] の確認ダイアログボックスで、[削除] を選択します。

チャンネルを削除するには

1. [チャンネル] ページで、削除するチャンネルを選択します。
2. [Delete] (削除) をクリックします。
3. [チャンネルの削除] の確認ダイアログボックスで、[削除] を選択します。

MediaPackage により、対象のチャンネルと、それに関連付けられているすべてのエンドポイントが削除されます。

# MediaPackage での live-to-VOD コンテンツ配信の開始

この入門チュートリアルでは、AWS Elemental MediaPackage コンソールを使用して Live-to-VOD (ビデオオンデマンド) アセットを作成し、再生可能にする方法を示します。

Live-to-VOD コンテンツを配信するには、以下の 3 つの主要な操作を行います。

- ライブ HLS コンテンツストリームを MediaPackage に取り込む
- ストリームから VOD アセットを抽出する
- アセットを再生可能にする

## Note

Live-to-VOD アセットを視聴者に配信するために MediaPackage を使用する必要はありません。このチュートリアルは、MediaPackage を使用して Live-to-VOD ワークフローを完了する方法を示すことを目的にしています。

以下のセクションは、これらの 3 つの操作とその他の補助操作を理解するためのガイド付きチュートリアルです。

## トピック

- [前提条件](#)
- [ステップ 1: MediaPackage にアクセスする](#)
- [ステップ 2: ライブコンテンツを取り込む](#)
- [ステップ 3: VOD アセットを抽出する](#)
- [\(オプション\) ステップ 4: VOD コンテンツを出力する](#)
- [\(オプション\) ステップ 5: MediaPackage のアクティビティをモニタリングする](#)
- [ステップ 6: クリーンアップする](#)

## 前提条件

AWS Elemental MediaPackage を使用するには、事前に AWS アカウントが必要です。また、MediaPackage コンポーネントにアクセスして表示や編集を行うための適切なアクセス許可が必要です。システム管理者が「[設定](#)」の以下の手順を完了したことを確認してから、このチュートリアルに戻ってください。

- AWS アカウントを作成するには、「[へのサインアップ AWS](#)」を参照してください。
- MediaPackage へのアクセスを管理者以外のロールに許可するには、「[ポリシーと管理者以外のロールの作成](#)」を参照してください。
- Live-to-VOD アセットを保存および取得するための、Amazon S3 バケットへのアクセスを MediaPackage に許可するには、「[他の AWS サービスへのアクセスを AWS Elemental MediaPackage に許可する](#)」を参照してください。

## ステップ 1: MediaPackage にアクセスする

IAM の認証情報を使用して、AWS Elemental MediaPackage コンソールにサインインします。

```
https://console.aws.amazon.com/mediapackage/
```

## ステップ 2: ライブコンテンツを取り込む

ライブコンテンツストリームを AWS Elemental MediaPackage に取り込み、そこからビデオオンデマンド (VOD) アセットを抽出するには、チャンネルとエンドポイントを作成します。チャンネルは MediaPackage へのエントリポイントであり、エンドポイントはストリームへのアクセスを MediaPackage に提供することで、VOD アセットを抽出できるようになります。以下の各セクションで、MediaPackage コンソールを使用してチャンネルとエンドポイントを作成する方法について説明します。

### チャンネルの作成

チャンネルは MediaPackage の最初のコンポーネントです。チャンネルは、AWS Elemental MediaLive などのエンコーダーからのライブコンテンツを受け取る、MediaPackage の入力に対応します。

MediaPackage に対しては、ユーザーが個人データを提供する必要はありません。お客様によるお客様データの供給が予想されるチャンネルにフィールドはありません。

### チャンネルを作成する

1. MediaPackage の [Channels] (チャンネル) ページで、[Create channel] (チャンネルの作成) をクリックします。
2. [ID] に、チャンネルを説明する名前として **channelHLS1** などと入力します。ID は、チャンネルのプライマリ識別子であり、AWS リージョン 内のアカウント別に一意である必要があります。使用できるのは、文字、数字、下線 (  )、ダッシュ (-) のみです。ID にスペースを使用することはできません。

3. 残りのフィールドはデフォルトのままにして、[作成] を選択します。

MediaPackage が、新しいチャンネルの詳細ページを表示します。

4. チャンネルの詳細ページで、[URL]、[ユーザー名]、[パスワード] の値をメモします。入力冗長を使用している場合、両方の入力 URL でこの情報が必要です。チャンネルに 1 つのストリームのみを送信する場合は、いずれかの入力 URL の情報をメモします。

WebDAV ユーザー名とパスワードは、チャンネルの作成時に MediaPackage により安全に生成されます。これらの認証情報を変更する必要がある場合は、「[入力 URL での認証情報の更新](#)」を参照してください。

以上のフィールドの情報をアップストリームエンコーダーの担当者に渡します。エンコーダーのストリーム設定で、この担当者は入力 URL として送信先を入力し、チャンネルのユーザー名およびパスワードとして WebDAV の認証情報を入力する必要があります。アップストリームエンコーダーは、ダイジェスト認証を使用して、HTTPS 経由で WebDAV を MediaPackage にプッシュし、その際、これらの認証情報を含める必要があります。入力冗長を使用している場合は、このチャンネルへの各入力ストリームのエンコーダ設定を同じにする必要があります。入力冗長のソースストリームの設定の詳細については、「[ライブ入力冗長の AWS Elemental MediaPackage 処理の流れ](#)」を参照してください。

## エンドポイントの作成

エンドポイントは、チャンネルにアタッチされ、ライブコンテンツの出力を表します。ライブコンテンツから VOD アセットを抽出する収集ジョブを作成するときに、抽出元のエンドポイントを指定する必要があります。クリアな (非暗号化の) エンドポイント、もしくは HLS と DASH の暗号化されたエンドポイントからアセットを収集することが可能です。このエンドポイントでは、スタートオーバーウィンドウが定義されている必要があります。暗号化されたエンドポイントしかない場合は、「[AWS Elemental MediaPackage を使用した live-to-VOD アセットの作成](#)」機能リファレンスを参照してください。

MediaPackage に対しては、ユーザーが個人データを提供する必要はありません。エンドポイントには、お客様自身によるお客様データの供給が予想されるフィールドはありません。

エンドポイントを作成するには

1. [Channels] (チャンネル) ページで、エンドポイントに関連付けるチャンネルを選択します。
2. チャンネルの詳細ページの [オリジンエンドポイント] で、[エンドポイントの管理] を選択します。

- [ID] に、エンドポイントを説明する名前として **HLSendpoint1** などと入力します。ID は、エンドポイントのプライマリ識別子であり、AWS リージョン 内のアカウントに対して一意である必要があります。使用できるのは、文字、数字、下線 (\_)、ダッシュ (-) のみです。ID にスペースを使用することはできません。
- 残りのフィールドはデフォルトのままにして、[Save (保存)] を選択します。

MediaPackage に、先に作成したエンドポイントを含む、チャンネルの詳細ページが表示されます。

- チャンネルの詳細ページで、エンドポイントの [URL] フィールドの値をメモします。この情報をダウンストリームデバイス (CDN またはプレーヤー) の担当者に渡します。この担当者は、ダウンストリームデバイスでエンドポイントの URL として、リクエスト送信先を入力する必要があります。

## ステップ 3: VOD アセットを抽出する

ライブコンテンツストリームから Live-to-VOD アセットを抽出するには、収集ジョブを作成します。収集ジョブは、アセットを収集するエンドポイント、アセットの開始時間と終了時間、および MediaPackage が収集したアセットを保存する場所を識別します。

収集ジョブを作成するには

- [ハーベストジョブ] ページで、[ハーベストジョブの作成] を選択します。
- [ID] に、収集ジョブを説明する名前 (**gamehighlights** など) を入力します。ID は収集ジョブの主要な識別子です。収集ジョブが期限切れになりアカウントから削除された後、そのジョブの ID は再利用できます。使用できるのは、文字、数字、下線 (\_)、ダッシュ (-) のみです。ID にスペースを使用することはできません。
- [Origin endpoint (配信エンドポイント)] で、VOD アセットを抽出するライブコンテンツストリームのエンドポイントを選択します。エンドポイントは、クリアな (暗号化されていない) コンテンツ、もしくは DASH か HLS の暗号化されたコンテンツを提供する必要があります。暗号化されたライブコンテンツから抽出する場合は、[「AWS Elemental MediaPackage を使用した live-to-VOD アセットの作成」](#)を参照してください。
- [Date and time format (日付と時刻の形式)] は、デフォルトのままにします。
- [When the live-to-VOD asset begins] と [When the live-to-VOD asset ends] に、抽出した VOD アセットの開始日時と終了日時を入力します。開始時刻は、ライブストリームの開始時刻後かつ現在の時刻 (「現在」) より前にすることをお勧めします。終了時間は過去であることが必要です。

**Note**

「現在」とは、エンコーダーからのソースコンテンツの EXT-X-PROGRAM-DATE-TIME に従った現在の時刻です。そのため、アップストリームエンコーダーでソースに EXT-X-PROGRAM-DATE-TIME タグを提供することをお勧めします。

- [IAM ロールの ARN] に、MediaPackage に対して Amazon S3 バケットへの live-to-VOD アセットの書き込みを許可する IAM ロールを入力します。ロールのヘルプについては、「[他の AWS サービスへのアクセスを AWS Elemental MediaPackage に許可する](#)」を参照してください。
- [Amazon S3 バケット名] で、MediaPackage によって live-to-VOD アセットが保存される Amazon S3 バケットを選択します。
- [マニフェストキー] に、live-to-VOD アセットの親マニフェストの Amazon S3 バケット内のパスと識別子を入力します。MediaPackage は、ここに入力したパスに基づいてディレクトリを作成します。

**Important**

マニフェストキーは一意であることが必要です。複数の収集ジョブに同じマニフェストキーを使用すると、アセットの最新の再生リストによって既存の再生リストが上書きされます。マニフェストキーを再利用する必要があるのは、コンテンツの前の収集に問題があった場合など、同じコンテンツを収集するときのみです。

- [Create] (作成) を選択します。

MediaPackage は収集ジョブを処理し、このジョブが失敗または成功した時点で CloudWatch イベントを送信します。イベントには、収集ジョブの詳細が含まれています。ジョブが失敗した場合、イベントには理由に関する情報が含まれます。この情報は、CloudWatch イベント内でのみ利用できます。イベントの例については、「[収集ジョブの通知イベント](#)」を参照してください。

## (オプション) ステップ 4: VOD コンテンツを出力する

MediaPackage を使用して Live-to-VOD アセットを再生可能にするには、パッケージンググループ、パッケージング設定、およびアセットリソースの作成を行います。アセットは、Amazon S3 バケットから Live-to-VOD アセットを取り込みます。パッケージンググループは、出力形式と設定を定義する 1 つ以上のパッケージング設定を保持します。



## パッケージンググループを作成する

パッケージンググループは、1つ以上のパッケージング設定を保持しています。パッケージ設定により、使用する VOD 出力の種類を定義することができます。これらの出力に関する定義を適用するには、パッケージンググループを複数のアセットに関連付けます。

### Example

15 種類のソースコンテンツが使用できます。これらすべてを DASH、HLS、および暗号化された HLS 出力として提供する場合を考えます。これを実行するためには、DASH、HLS、および暗号化された HLS を使用する 1 つのパッケージンググループを、パッケージ設定で定義します。その後、定義したグループを、コンテンツのこれらの各部に対応したアセットリソースに関連付けます。アセットごとに新しく設定を作成する必要はありません。

MediaPackage に対して、顧客データを提供する必要はありません。パッケージンググループには、顧客データの提供をユーザーに求めるようなフィールドはありません。

パッケージンググループを作成するには

1. [パッケージグループ] ページで [グループを作成] を選択します。
2. [ID] に、グループの説明となるような名前 (**gamehighlights** など) を入力します。ID は、グループのプライマリ識別子であり、この AWS リージョン 内のアカウントに対して一意である必要があります。使用できるのは、文字、数字、下線 (  )、ダッシュ (-) のみです。ID にスペースを使用することはできません。
3. [Create] (作成) を選択します。

## パッケージング設定を作成する

パッケージ設定は、ストリーム選択の制限や順序など、出力マニフェストの設定方法を指定します。

MediaPackage に対しては、ユーザーが個人データを提供する必要はありません。パッケージング設定には、顧客データの提供をユーザーに求めるようなフィールドはありません。

パッケージング設定を作成するには

1. [Packaging groups (パッケージンググループ)] ページで、作成したグループを選択します。
2. パッケージグループの詳細ページの、[パッケージ設定] で、[設定を管理] を選択します。
3. [パッケージ設定を管理] ページで、[追加]、[新しい設定] の順に選択します。

- [ID] に、設定を説明する名前として **hls\_highlights** などと入力します。ID は、設定のプライマリ識別子であり、この AWS リージョン 内のアカウントに対して一意である必要があります。使用できるのは、文字、数字、下線 (\_)、ダッシュ (-) のみです。ID にスペースを使用することはできません。
- 残りのフィールドはデフォルトのままにして、[Save (保存)] を選択します。

## アセットを作成する

アセットリソースにより、AWS Elemental MediaPackage が VOD コンテンツを取り込み、パッケージ化し、提供する方法が決定します。アセットは、1 つ以上のパッケージング設定に関連付けられます。ダウンロードデバイスが、アセット上の特定のパッケージング設定に対し、再生リクエストを送信します。

MediaPackage はユーザーからの顧客データを必要としないため、アセットにはそれらのフィールドは含まれません。

アセットを作成してソースコンテンツを取り込むには

- Amazon S3 バケット内で、ソースコンテンツに使用しているファイルを特定します。以下の情報を記録します。
  - ファイルが保存されている Amazon S3 バケットの名前
  - S3://bucket/path/source-file-name などのファイルの完全パス
  - MediaPackage に Amazon S3 からの読み取りを許可する IAM ロール
- MediaPackage コンソールで、[アセット] ページにアクセスして、[アセットを取り込む] を選択します。
- [Amazon S3 バケット名] で、ソースコンテンツを保存するバケットを選択します。
- [IAM ロール] で、[既存のロールを使用] をクリックして、MediaPackage に Amazon S3 からの読み取りを許可する IAM ロールを選択します。
- [Filename] (ファイル名) に、Amazon S3 バケット内の [.smil マニフェスト](#) (MP4) または m3u8 親プレイリスト (HLS) への完全なパスを、ソースコンテンツの名前を含めながら入力します。例えば、lion\_movie.m3u8 という名前のコンテンツが、movies という名前のバケット内の thursday\_night というサブディレクトリに置かれている場合は、次のように [ファイル名] フィールドに入力します。

```
thursday_night/lion_movie.m3u8
```



[Amazon S3 バケット名] フィールドで選択したため、バケット名を入力する必要はありません。

6. [パッケージグループ] で、[パッケージンググループを作成する](#) で作成したグループを選択します。
7. [アセットの取り込み] を選択します。

## 再生 URL を指定する

アセットリソースの作成が終わると、AWS Elemental MediaPackage はパッケージ化されたマニフェストを視聴者に提供するための準備を行います。これはバックグラウンドで行われ、ソースコンテンツのサイズと複雑さによっては時間がかかる場合がありますが、通常は数分以内です。マニフェストの URL はアセットの詳細ページですぐに利用できますが、コンテンツはまだ再生できません。

各マニフェストの処理が完了すると、MediaPackage はユーザーのアカウントに、Amazon CloudWatch イベントを送信します。

各パッケージング設定の URL は、MediaPackage によりアセット上に記述されています。この URL を使用して、ダウンストリームデバイス (CDN または再生デバイス) は MediaPackage に対し、VOD コンテンツをリクエストします。

再生 URL を取得するには

1. MediaPackage コンソールで [Assets] (アセット) ページを開き、「[ステップ 4: アセットを作成する](#)」で作成したアセットの [ID] を選択します。
2. アセットの詳細ページで、各パッケージング設定の URL を取得します。
3. この URL をダウンストリームデバイス (CDN またはプレーヤー) の担当者に渡します。ダウンストリームデバイスでは、この担当者は対応するパッケージ設定からの URL としてリクエスト先を入力する必要があります。

各 URL は安定しています。このアセットとパッケージング設定の組み合わせの有効期間中に変更されることはありません。この URL をダウンストリームデバイス (CDN またはプレーヤー) の担当者に渡します。この担当者は、ダウンストリームデバイスでアセットの URL として、リクエスト送信先を入力する必要があります。

## (オプション) ステップ 5: MediaPackage のアクティビティをモニタリングする

Amazon CloudWatch を使用して、MediaPackage によるアクティビティ (MediaPackage が受信/送信したバイト数、応答時間、リクエスト数など) を追跡します。メトリクスはまずサービスの名前空間ごとにグループ化され、次に各名前空間内のさまざまなディメンションの組み合わせごとにグループ化されます。

CloudWatch コンソールを使用してメトリクスを表示するには

1. CloudWatch コンソール (<https://console.aws.amazon.com/cloudwatch/>) を開きます。
2. ナビゲーションペインで [Metrics] (メトリクス) を選択します。
3. [All metrics] (すべてのメトリクス) で、[AWS/MediaPackage] 名前空間を選択します。
4. メトリクスディメンションを選択してメトリクスを表示します (たとえば、channel を選択してチャンネル別にメトリクスを表示します)。

MediaPackage でのメトリクスの一覧は、「[Amazon CloudWatch メトリクス AWS Elemental MediaPackage によるモニタリング](#)」でご確認ください。

## ステップ 6: クリーンアップする

追加料金が発生しないように、使用しなくなったリソースを削除します。

### Note

期限切れになった収集ジョブは自動的にアカウントから削除されます。手動で削除することはできません。

## ライブリソースを削除する

ライブコンテンツの取り込み、提供、収集が完了したら、チャンネルとエンドポイントを削除します。チャンネルのすべてのエンドポイントを削除すると、チャンネル自体を削除できます。

エンドポイントを削除するには

1. MediaPackage の [チャンネル] ページで、エンドポイントが関連付けられているチャンネルを選択します。

2. チャンネルの詳細ページの [オリジンエンドポイント] で、削除するオリジンエンドポイントを選択します。
3. [削除] を選択します。
4. [エンドポイントの削除] の確認ダイアログボックスで、[削除] を選択します。

#### チャンネルを削除するには

1. [チャンネル] ページで、削除するチャンネルを選択します。
2. [Delete] (削除) をクリックします。
3. [チャンネルの削除] の確認ダイアログボックスで、[削除] を選択します。

MediaPackage により、対象のチャンネルと、それに関連付けられているすべてのエンドポイントが削除されます。

#### VOD リソースを削除する

VOD コンテンツの取り込みと提供が完了したら、余分なリソースを削除します。特定の出力を利用できないようにする場合は、パッケージンググループからパッケージング設定を削除します。アセットをどの出力からも再生できないようにする場合は、そのアセットを削除します。

#### アセットを削除するには

1. MediaPackage コンソールで、[アセット] ページにアクセスして、アセットの [ID] を選択します。
2. アセットの詳細ページで、[Delete (削除)] を選択します。
3. 確認ダイアログボックスで、[削除] を選択します。

#### パッケージング設定を削除するには

1. MediaPackage コンソールで、[パッケージグループ] ページにアクセスします。
2. 削除する設定を持つグループの [ID] を選択します。
3. パッケージンググループの詳細ページの、[Packaging configurations (パッケージング設定)] セクションで、設定を見つけけて [ID] を選択します。
4. パッケージング設定の詳細ページで、[Delete (削除)] を選択します。
5. 確認ダイアログボックスで、[削除] を選択します。

# MediaPackage での VOD コンテンツの配信開始

この入門チュートリアルでは、AWS Elemental MediaPackage コンソールを使用してビデオオンデマンド (VOD) コンテンツを取り込み、再生できるようにする方法を説明します。

## トピック

- [前提条件](#)
- [ステップ 1: MediaPackage にアクセスする](#)
- [ステップ 2: パッケージンググループの作成](#)
- [ステップ 3: パッケージング設定を作成する](#)
- [ステップ 4: アセットを作成する](#)
- [ステップ 5: 再生 URL を指定する](#)
- [\(オプション\) ステップ 6: MediaPackage のアクティビティをモニタリングする](#)
- [ステップ 7: クリーンアップする](#)

## 前提条件

AWS Elemental MediaPackage VOD 機能を使用するには、事前に次の条件を満たしている必要があります。

- AWS アカウントと MediaPackage コンポーネントにアクセスし、表示や編集を行うための適切なアクセス許可を持っている。システム管理者が [設定](#) の手順を完了したことを確認してから、このチュートリアルに戻ってください。
- 1 つ以上の Amazon S3 バケット内にファイルベースのソースコンテンツが用意されている。

サポートされている VOD 入力とコーデックについては、「[VOD でサポートされるコーデックおよび入力タイプ](#)」を参照してください。

## ステップ 1: MediaPackage にアクセスする

IAM の認証情報を使用して、AWS Elemental MediaPackage コンソールにサインインします。

```
https://region.console.aws.amazon.com/mediapackage/home
```

## ステップ 2: パッケージンググループの作成

パッケージンググループは、1 つ以上のパッケージング設定を保持しています。パッケージ設定により、使用する VOD 出力の種類を定義することができます。これらの出力に関する定義を適用するには、パッケージンググループを複数のアセットに関連付けます。

### Example

15 種類のソースコンテンツが使用できます。これらすべてを DASH、HLS、および暗号化された HLS 出力として提供する場合を考えます。これを実行するためには、DASH、HLS、および暗号化された HLS を使用する 1 つのパッケージンググループを、パッケージ設定で定義します。その後、定義したグループを、コンテンツのこれらの各部に対応したアセットリソースに関連付けます。アセットごとに新しく設定を作成する必要はありません。

MediaPackage に対して、顧客データを提供する必要はありません。パッケージンググループには、顧客データの提供をユーザーに求めるようなフィールドはありません。

パッケージンググループを作成するには

1. [パッケージグループ] ページで [グループを作成] を選択します。
2. [ID] に、グループの説明となるような名前 (**gamehighlights** など) を入力します。ID は、グループのプライマリ識別子であり、この AWS リージョン 内のアカウントに対して一意である必要があります。使用できるのは、文字、数字、下線 (\_)、ダッシュ (-) のみです。ID にスペースを使用することはできません。
3. [Create] (作成) を選択します。

## ステップ 3: パッケージング設定を作成する

パッケージ設定は、ストリーム選択の制限や順序など、出カマニフェストの設定方法を指定します。

MediaPackage に対しては、ユーザーが個人データを提供する必要はありません。パッケージング設定には、顧客データの提供をユーザーに求めるようなフィールドはありません。

パッケージング設定を作成するには

1. [Packaging groups (パッケージンググループ)] ページで、作成したグループを選択します。
2. パッケージグループの詳細ページの、[パッケージ設定] で、[設定を管理] を選択します。
3. [パッケージ設定を管理] ページで、[追加]、[新しい設定] の順に選択します。

- [ID] に、設定を説明する名前として **hls\_highlights** などと入力します。ID は、設定のプライマリ識別子であり、この AWS リージョン 内のアカウントに対して一意である必要があります。使用できるのは、文字、数字、下線 (\_)、ダッシュ (-) のみです。ID にスペースを使用することはできません。
- 残りのフィールドはデフォルトのままにして、[Save (保存)] を選択します。

## ステップ 4: アセットを作成する

アセットリソースにより、MediaPackage が VOD コンテンツを取り込み、パッケージ化し、提供する方法が決定します。アセットは、1 つ以上のパッケージング設定に関連付けられます。ダウンストリームデバイスが、アセット上の特定のパッケージング設定に対し、再生リクエストを送信します。

MediaPackage はユーザーからの顧客データを必要としないため、アセットにはそれらのフィールドは含まれません。

アセットを作成するには

- Amazon S3 バケット内で、ソースコンテンツに使用しているファイルを特定します。以下の情報を記録します。
  - ファイルが保存されている Amazon S3 バケットの名前
  - S3://bucket/path/source-file-name などのファイルの完全パス
  - MediaPackage に Amazon S3 からの読み取りを許可する IAM ロール
- MediaPackage コンソールで、[アセット] ページにアクセスして、[アセットを取り込む] を選択します。
- [Amazon S3 バケット名] で、ソースコンテンツを保存するバケットを選択します。
- [IAM ロール] で、[既存のロールを使用] をクリックして、MediaPackage に Amazon S3 からの読み取りを許可する IAM ロールを選択します。
- [Filename] (ファイル名) に、Amazon S3 バケット内の .smil マニフェスト (MP4) または .m3u8 親プレイリスト (HLS) への完全なパスを、ソースコンテンツの名前を含めながら入力します。[Amazon S3 バケット名] フィールドで選択したため、バケット名を入力する必要はありません。例えば、lion\_movie.m3u8 という名前のコンテンツが、movies という名前のバケット内の thursday\_night というサブディレクトリに置かれている場合は、次のように [Filename] (ファイル名) フィールドに入力します。

```
thursday_night/lion_movie.m3u8
```

MediaPackage で .smil マニフェストを使用する方法の詳細については、「[.smil マニフェストでの要件](#)」を参照してください。

6. [パッケージグループ] で、[ステップ 2: パッケージンググループの作成](#) で作成したグループを選択します。
7. [アセットの取り込み] を選択します。

## ステップ 5: 再生 URL を指定する

アセットリソースの作成が終わると、AWS Elemental MediaPackage はパッケージ化されたマニフェストを視聴者に提供するための準備を行います。これはバックグラウンドで行われ、ソースコンテンツのサイズと複雑さによっては時間がかかる場合がありますが、通常は数分以内です。マニフェストの URL はアセットの詳細ページですぐに利用できますが、コンテンツはまだ再生できません。

各マニフェストの処理が完了すると、MediaPackage はユーザーのアカウントに、Amazon CloudWatch イベントを送信します。

各パッケージング設定の URL は、MediaPackage によりアセット上に記述されています。この URL を使用して、ダウンストリームデバイス (CDN または再生デバイス) は MediaPackage に対し、VOD コンテンツをリクエストします。

再生 URL を取得するには

1. MediaPackage コンソールで [Assets] (アセット) ページを開き、「[ステップ 4: アセットを作成する](#)」で作成したアセットの [ID] を選択します。
2. アセットの詳細ページで、各パッケージング設定の URL を取得します。
3. この URL をダウンストリームデバイス (CDN またはプレーヤー) の担当者に渡します。ダウンストリームデバイスでは、この担当者は対応するパッケージ設定からの URL としてリクエスト先を入力する必要があります。

各 URL は安定しています。このアセットとパッケージング設定の組み合わせの有効期間中に変更されることはありません。この URL をダウンストリームデバイス (CDN またはプレーヤー) の担当者に渡します。この担当者は、ダウンストリームデバイスでアセットの URL として、リクエスト送信先を入力する必要があります。



## (オプション) ステップ 6: MediaPackage のアクティビティをモニタリングする

Amazon CloudWatch を使用して、MediaPackage によるアクティビティ (MediaPackage が受信/送信したバイト数、応答時間、リクエスト数など) を追跡します。メトリクスはまずサービスの名前空間ごとにグループ化され、次に各名前空間内のさまざまなディメンションの組み合わせごとにグループ化されます。

CloudWatch コンソールを使用してメトリクスを表示するには

1. CloudWatch コンソール (<https://console.aws.amazon.com/cloudwatch/>) を開きます。
2. ナビゲーションペインで [Metrics] (メトリクス) を選択します。
3. [All metrics] (すべてのメトリクス) で、[AWS/MediaPackage] 名前空間を選択します。
4. メトリクスディメンションを選択してメトリクスを表示します (たとえば、channel を選択してチャンネル別にメトリクスを表示します)。

MediaPackage でのメトリクスの一覧は、「[AWS Elemental MediaPackage VOD コンテンツメトリクス](#)」でご確認ください。

## ステップ 7: クリーンアップする

追加料金の発生を避けるには、VOD リソースを削除します。特定の出力を利用できないようにする場合は、パッケージンググループからパッケージング設定を削除します。アセットをどの出力からも再生できないようにする場合は、そのアセットを削除します。

アセットを削除するには

1. MediaPackage コンソールで、[アセット] ページにアクセスして、アセットの [ID] を選択します。
2. アセットの詳細ページで、[Delete (削除)] を選択します。
3. 確認ダイアログボックスで、[削除] を選択します。

パッケージング設定を削除するには

1. MediaPackage コンソールで、[パッケージグループ] ページにアクセスします。
2. 削除する設定を持つグループの [ID] を選択します。



3. パッケージンググループの詳細ページの、[Packaging configurations (パッケージング設定)] セクションで、設定を見つけて [ID] を選択します。
4. パッケージング設定の詳細ページで、[Delete (削除)] を選択します。
5. 確認ダイアログボックスで、[削除] を選択します。

# AWS Elemental MediaPackage からのライブコンテンツの配信

AWS Elemental MediaPackage はライブコンテンツに次のリソースを使用します。

- チャンネルは、アップストリームエンコーダーからのライブストリームのエントリポイントです。  
サポートされているライブ入力とコーデックについては、「[ライブでサポートされるコーデックおよび入力タイプ](#)」を参照してください。。
- エンドポイントは、アウトバウンドコンテンツをパッケージ化する方法を MediaPackage に指示します。エンドポイントはチャンネルに関連付けられており、暗号化、ストリーム、およびパッケージ設定を保持します。

以下の各セクションで、これらのリソースを使用して MediaPackage のライブコンテンツを管理する方法について説明します。

## トピック

- [AWS Elemental MediaPackage でチャンネルを使用する](#)
- [AWS Elemental MediaPackage でエンドポイントを使用する](#)

## AWS Elemental MediaPackage でチャンネルを使用する

チャンネルは、AWS Elemental MediaLive や他のエンコーダーなどのソースからライブコンテンツストリームを AWS Elemental MediaPackage (MediaPackage) で受け取るのに必要なすべての情報を保持します。チャンネルは、コンテンツを受け取ってパッケージ化し、エンドポイントを通じてリクエスト元のダウンストリームデバイス (ビデオプレーヤーや CDN など) にコンテンツを出力します。

チャンネルが作成されると、MediaPackage は、チャンネルの存続期間にわたって不変の入力 URL のペアを生成します。この入力 URL は、後にアップグレードや障害が発生した場合でも、変更されることはありません。アップストリームエンコーダーの出力は、MediaPackage へのストリーム配信の URL に伝送されます。

サポートされているライブ入力とコーデックについては、「[ライブでサポートされるコーデックおよび入力タイプ](#)」を参照してください。。

## トピック

- [チャンネルの作成](#)
- [チャンネルの詳細の表示](#)
- [チャンネルの編集](#)
- [入力 URL での認証情報の更新](#)
- [チャンネルの削除](#)
- [チャンネルへのエンドポイントの追加](#)

## チャンネルの作成

ストリームコンテンツの受信を開始するには、チャンネルを作成します。後で、チャンネルにエンドポイントを追加します。このエンドポイントは、コンテンツ再生リクエストのアクセスポイントです。

チャンネルを作成するには、AWS Elemental MediaPackage コンソール、AWS CLI、MediaPackage API を使用できます。AWS CLI または MediaPackage API を使用したチャンネルの作成方法については、[AWS Elemental MediaPackage API リファレンス](#)を参照してください。

チャンネルの作成中に、[名前] フィールドのような自由記述のフィールドに顧客アカウント番号などの機密扱いの識別情報を入力しないようにしてください。これは、MediaPackage コンソール、MediaPackage API、AWS CLI、AWS SDK を使用して MediaPackage を操作する場合も同様です。MediaPackage に入力するデータはすべて、取得され、診断ログもしくは Amazon CloudWatch Events に包含される場合があります。

チャンネルを作成するには (コンソール)

1. MediaPackage コンソール (<https://console.aws.amazon.com/mediapackage/>) を開きます。
2. ナビゲーションペインの [ライブ] で、[チャンネル] を選択します。
3. [Channels] (チャンネル) ページで、[Create channel] (チャンネルの作成) を選択します。
4. [ID] に、チャンネルを記述する名前を入力します。ID は、チャンネルのプライマリ識別子であり、リージョン内のアカウント別に一意であることが必要です。
5. (オプション) [説明] に、チャンネルを特定する際に手掛かりとなる説明テキストを入力します。
6. [Input type] (入力タイプ) で、[Apple HLS] を選択します。
7. [Create] (作成) を選択します。

MediaPackage が、新しいチャンネルの詳細ページを表示します。

このチャンネルはアクティブな状態なので、コンテンツが作成されると、すぐにその受信を開始できます。MediaPackage は、トラフィックに合わせて適切な容量が使用できるよう、リソースをスケールアップまたはスケールダウンします。入力冗長を使用していて、いずれかの入力からのコンテンツが停止した場合、MediaPackage は、ソースコンテンツに接続された別の入力に自動的に切り替えます。入力冗長の仕組みの詳細については、「[ライブ入力冗長の AWS Elemental MediaPackage 処理の流れ](#)」を参照してください。

チャンネルの作成時にアカウントのクォータを超えた場合は、エラーが発生します。この際のエラーは、「リクエストが多すぎます。もう一度お試しください。」といった内容です。リソース制限を超過したと言うのは、API リクエストの数がクォータを超過したか、チャンネルの数がアカウントで使用できる上限に既に到達していることを意味します。これが最初のチャンネルであるか、このエラーが誤って表示されたと思われる場合は、Service Quotas コンソールを使用して、[クォータの引き上げをリクエスト](#)してください。MediaPackage でのクォータの詳細については、「[AWS Elemental MediaPackage のクォータ](#)」を参照してください。

## チャンネルの詳細の表示

AWS Elemental MediaPackage に設定されているすべてのチャンネルを表示します。または、特定のチャンネルの詳細 (関連付けられているエンドポイントなど) を表示します。

チャンネルの詳細を表示するには、MediaPackage コンソール、AWS CLI、MediaPackage API を使用できます。AWS CLI または MediaPackage API を使用してチャンネルの詳細を表示する方法については、[AWS Elemental MediaPackage API リファレンス](#)を参照してください。

チャンネルを表示するには (コンソール)

1. MediaPackage コンソール (<https://console.aws.amazon.com/mediapackage/>) を開きます。
2. [チャンネル] ページが表示されない場合は、MediaPackage のホームページで [スキップしてコンソールに移動] を選択します。

すべての既存のチャンネルがコンソールに表示されます。

3. (オプション) 表示設定 (表示するページのサイズやプロパティなど) を調整するには、[詳細設定] を選択します。
4. 特定のチャンネルに関する詳細情報を表示するには、そのチャンネルの名前を選択します。

MediaPackage により、[入力 URL] の値や、各入力 URL における WebDAV の [ユーザー名] および [パスワード] の値など、重要な情報が表示されます。これらの情報をアップストリームエ

ンコーダーのストリーム送信先設定として指定します。入力冗長を使用している場合、両方の入力 URL の情報が提供されます。チャンネルに 1 つのストリームのみを送信する場合は、いずれかの入力 URL の情報を提供できます。入力冗長の仕組みについては、「[ライブ入力冗長の AWS Elemental MediaPackage 処理の流れ](#)」を参照してください。

#### Note

すべてのチャンネルには 2 つの入力 URL があります。入力冗長以前に存在していたチャンネルについては、新しい 2 つの入力 URL が MediaPackage により作成されます。チャンネルへの入力には新旧の URL のいずれかを使用できます。親マニフェストには **channel.m3u8** という名前を付ける必要があります。

MediaPackage コンソールで Amazon CloudFront ディストリビューションを作成した場合、チャンネルからは、ディストリビューションの概要情報 (ステータスや ID など) が確認できるようになります。MediaPackage でエンドポイントを追加すると、ディストリビューションにはオリジンが追加され、また、チャンネルの詳細ページに CloudFront の CDN URL が表示されるようになります。

## チャンネルの編集

チャンネルの説明を編集し、後でわかりやすい内容に変えます。

AWS Elemental MediaPackage コンソールからは、チャンネルの説明を編集したり、Amazon CloudFront のディストリビューションの作成を有効化したりできます。

#### Note

既存のディストリビューション (MediaPackage から作成したものも含む) を変更するには、Amazon CloudFront コンソールに移動します。

チャンネルを編集するには、MediaPackage コンソール、AWS CLI、MediaPackage API を使用できます。AWS CLI または MediaPackage API を使用してチャンネルを編集する方法については、[AWS Elemental MediaPackage API リファレンス](#)を参照してください。

チャンネルの編集中に、[名前] フィールドのような自由記述のフィールドに顧客アカウント番号などの機密扱いの識別情報を入力しないようにしてください。これは、MediaPackage コンソール

ル、MediaPackage API、AWS CLI、AWS SDK を使用して MediaPackage を操作する場合も同様です。MediaPackage に入力するデータはすべて、取得され、診断ログもしくは Amazon CloudWatch Events に包含される場合があります。

チャンネルを編集するには (コンソール)

1. MediaPackage コンソール (<https://console.aws.amazon.com/mediapackage/>) を開きます。
2. [チャンネル] ページが表示されない場合は、MediaPackage のホームページで [スキップしてコンソールに移動] を選択します。
3. [Channels] (チャンネル) ページで、編集するチャンネルの名前を選択します。
4. チャンネルの詳細ページで、[編集] を選択します。
5. 必要な変更を行います。
6. [更新] を選択します。

## 入力 URL での認証情報の更新

入力 URL で認証情報を更新して、新しい WebDAV ユーザー名とパスワードを生成します。

認証情報を更新するには、AWS Elemental MediaPackage コンソールまたは MediaPackage API を使用できます。MediaPackage API で認証情報を更新する方法については、[AWS Elemental MediaPackage API リファレンス](#) を参照してください。

認証情報を更新するには (コンソール)

1. MediaPackage コンソール (<https://console.aws.amazon.com/mediapackage/>) を開きます。
2. [チャンネル] ページが表示されない場合は、MediaPackage のホームページで [スキップしてコンソールに移動] を選択します。
3. [Channels (チャンネル)] ページで、認証情報を更新する入力 URL を保持しているチャンネルの名前を選択します。
4. チャンネルの詳細ページで、認証情報を更新する入力 URL を選択してから、[Rotate credentials (認証情報の更新)] を選択します。
5. 新しいユーザー名とパスワードの生成を確定するには、[Rotate (更新)] を選択します。

MediaPackage により、新しい認証情報が表示されます。

## チャンネルの削除

AWS Elemental MediaPackage でのコンテンツの受信を停止するには、チャンネルを削除します。チャンネルを削除する前に、チャンネルのエンドポイントを削除 ([「エンドポイントの削除」](#)を参照) する必要があります。

チャンネルの削除には、MediaPackage コンソール、AWS CLI、MediaPackage API を使用できます。AWS CLI または MediaPackage API を使用してチャンネルを削除する方法については、[AWS Elemental MediaPackage API リファレンス](#)を参照してください。

チャンネルを削除するには (コンソール)

1. MediaPackage コンソール (<https://console.aws.amazon.com/mediapackage/>) を開きます。
2. [チャンネル] ページが表示されない場合は、MediaPackage のホームページで [スキップしてコンソールに移動] を選択します。
3. [チャンネル] ページで、削除するチャンネルの名前を選択します。
4. [Delete] (削除) をクリックします。

チャンネルに関連付けられている Amazon CloudFront デイストリビューションが存在する場合は、確認ダイアログボックスで CloudFront へのリンクを選択し、CloudFront コンソールに移動してデイストリビューションを削除します。チャンネルを削除しても、MediaPackage はデイストリビューションを削除しません。CloudFront でのデイストリビューション削除については、Amazon CloudFront デベロッパーガイドの「[デイストリビューションを削除する](#)」を参照してください。

5. MediaPackage の確認ダイアログボックスで [削除] を選択してチャンネルを削除します。

## チャンネルへのエンドポイントの追加

チャンネルにエンドポイントを追加することで、ダウンストリームの動画プレイヤーやコンテンツ配信ネットワーク (CDN) はコンテンツ再生のリクエストを開始できます。

エンドポイントをチャンネルに追加するには、AWS Elemental MediaPackage コンソール、AWS CLI、MediaPackage API を使用できます。AWS CLI または MediaPackage API を使用した追加方法については、[AWS Elemental MediaPackage API リファレンス](#)を参照してください。

MediaPackage コンソールを使用してエンドポイントをチャンネルに追加する手順については、「[the section called “エンドポイントの使用”](#)」を参照してください。



# AWS Elemental MediaPackage でエンドポイントを使用する

エンドポイントは、チャンネルの単一の配信ポイントを定義します。エンドポイントには、AWS Elemental MediaPackage をプレイヤーや Amazon CloudFront などのコンテンツ配信ネットワークと統合するために必要なすべての情報が保持されます。エンドポイントは、以下のいずれかのストリーム形式で出力コンテンツに設定します。

- Apple HLS – コンテンツを Apple HTTP Live Streaming (HLS) 用にパッケージ化
- Microsoft Smooth Streaming – コンテンツを Microsoft Smooth Streaming プレイヤー用にパッケージ化
- DASH-ISO – コンテンツを DASH-ISO ABR ストリーミングプロトコル用にパッケージ化
- CMAF – コンテンツを Apple HLS fragmented MP4 (fMP4) をサポートするデバイス用にパッケージ化

さらに、エンドポイントにはデジタル著作権管理 (DRM)、暗号化統合、ストリームのビットレートの表示順などに関する情報も保持されます。

## トピック

- [エンドポイントの作成](#)
- [チャンネルに関連付けられたすべてのエンドポイントの表示](#)
- [単一のエンドポイントの表示](#)
- [エンドポイントの編集](#)
- [エンドポイントの削除](#)
- [エンドポイントのプレビュー](#)

## エンドポイントの作成

チャンネルでエンドポイントを作成し、AWS Elemental MediaPackage で配信用のコンテンツを準備する方法を定義します。チャンネルにエンドポイントを設定するまで、チャンネルからコンテンツを利用することはできません。入力冗長を使用している場合は、各エンドポイントが 1 度に 1 つの入力 URL からコンテンツを受信します。MediaPackage が 1 つの入力 URL で入力のフェイルオーバーを実行すると、エンドポイントでは、異なる入力 URL からのコンテンツの受信が自動的に開始されます。入力冗長とフェイルオーバーの詳細については、「[ライブ入力冗長の AWS Elemental MediaPackage 処理の流れ](#)」を参照してください。



エンドポイントを作成すると、エンドポイントの存続期間にわたって不変のパブリック URL が MediaPackage から割り当てられます。このパブリック URL は、途中で障害やアップグレードが発生した場合にも変更されません。プレイヤーや CDN は、この URL に従ってエンドポイントからストリームにアクセスします。

エンドポイントの作成には、MediaPackage コンソール、AWS CLI、MediaPackage API を使用できます。AWS CLI または MediaPackage API を使用してエンドポイントを作成する方法については、[AWS Elemental MediaPackage API リファレンス](#)を参照してください。

MediaPackage はユーザーからの顧客データを必要としないため、エンドポイントにはそれらのフィールドが含まれません。

## トピック

- [HLS エンドポイントの作成](#)
- [DASH エンドポイントの作成](#)
- [Microsoft Smooth Streaming エンドポイントの作成](#)
- [CMAF エンドポイントの作成](#)

## HLS エンドポイントの作成

Apple HLS をサポートするデバイス向けにコンテンツをフォーマットするエンドポイントを作成します。

Apple HLS エンドポイントを作成するには (コンソール)

1. エンドポイントに関連付けるチャンネルにアクセスします。手順については、「[チャンネルの詳細の表示](#)」を参照してください。
2. チャンネルの詳細ページの [オリジンエンドポイント] で、[エンドポイントの管理] を選択します。
3. 以下のトピックの説明に従ってフィールドに入力します。
  - [エンドポイントでの新しいフィールド](#)
  - [パッケージ設定のフィールド](#)
  - [パッケージの暗号化フィールド](#)
  - [アクセスコントロールの設定フィールド](#)
  - [ストリーム選択に関するフィールド](#)
4. [Save (保存)] を選択します。

AWS Elemental MediaPackage コンソールからの Amazon CloudFront デистриビューションの作成を有効化しており、チャンネルに初めてエンドポイントを作成した場合は、MediaPackage によって、このデистриビューションにオリジンが追加されます。CloudFront での CDN の URL とエンドポイントの情報は、チャンネルの詳細ページにあるエンドポイントセクションで確認できます。

エンドポイントがアクティブになり、その URL のエンドポイントにリクエストが送信されると、すぐにコンテンツを配信できます。MediaPackage は、トラフィックに合わせて適切な容量が使用できるよう、リソースをスケールアップまたはスケールダウンします。

エンドポイントの作成時にアカウントのクォータを超過した場合は、エラーが発生します。この際のエラーは、「リクエストが多すぎます。もう一度お試しください。」といった内容です。「リソース上限の超過」とは、API リクエストのクォータを超過しているか、エンドポイントの数がチャンネルで使用できる上限に既に到達していることを意味しています。このエラーが誤って表示されたと思われる場合は、Service Quotas コンソールを使用して、[クォータの引き上げをリクエスト](#)してください。MediaPackage でのクォータの詳細については、「[AWS Elemental MediaPackage のクォータ](#)」を参照してください。

## エンドポイントでの新しいフィールド

エンドポイントの作成中に、[名前] フィールドのような自由記述のフィールドに顧客アカウント番号などの機密扱いの識別情報を入力しないようにしてください。これは、MediaPackage コンソール、MediaPackage API、AWS CLI、AWS SDK を使用して AWS Elemental MediaPackage を操作する場合も同様です。MediaPackage に入力するデータはすべて、取得され、診断ログもしくは Amazon CloudWatch Events に包含される場合があります。

1. [ID] に、エンドポイントの説明となるような名前を入力します。ID はエンドポイントのプライマリ識別子であり、AWS リージョン 内のアカウントに対して一意である必要があります。
2. (オプション) [説明] に、エンドポイントを特定する際に手掛かりとなる説明テキストを入力します。
3. [Manifest name] (マニフェスト名) に、エンドポイント URL の末尾に付加する短い文字列を入力します。マニフェスト名により、このエンドポイントへの一意のパスを作成できます。
4. (オプション) [スタートオーバーウィンドウ] に、ウィンドウのサイズ (秒単位) を入力して、オンデマンド表示に利用できるライブストリームのウィンドウを作成します。視聴者は、ウィンドウ範囲内のコンテンツのスタートオーバーまたはキャッチアップを行うことができます。スタート

オーバーとキャプアップ TV の実装の詳細については、「[AWS Elemental MediaPackage のタイムシフト表示のリファレンス](#)」を参照してください。

5. (オプション) [時間遅延] に、遅延時間 (秒単位) を入力して、プレイヤーでコンテンツを利用できるようになる時間を遅らせます。最小の設定時間は 5 秒間です。最大時間は 86,400 秒 (24 時間) です。

時間遅延を使用してライブポイントを再定義し、「現在」の時刻から指定した遅延を差し引いた時刻にコンテンツを利用可能にします。例えば、時間遅延を 60 秒に設定している場合、MediaPackage が 12:20 に受信したコンテンツは 12:21 まで利用できません。12:20 の再生リクエストに対しては、12:19 のコンテンツが提供されます。同様に、タイムゾーンをまたいで提供するコンテンツの場合、タイムゾーンの時差に等しい時間遅延を設定することで、たとえば現地時間の 8:00 にコンテンツを提供できます。

遅延時間とスタートオーバーウィンドウを併用する場合は、時間遅延をスタートオーバーウィンドウより短くする必要があります。

#### Tip

短い出力セグメントで入力の冗長性を利用している場合は、時間遅延を使用することで、入力スイッチング時のバッファリング量を低減できます。遅延により、コンテンツ再生時のレイテンシーが増加する可能性があることに注意してください。

## パッケージ設定のフィールド

パッケージ設定のフィールドには、エンドポイントに関する一般的な情報を保持します。

1. [パッケージタイプ] で、[Apple HLS] を選択します。
2. (オプション) [Segment duration (セグメント時間)] に、各セグメントの時間 (秒単位) を入力します。入力セグメントの長さと同じか、その倍数の値を入力します。入力した値が入力セグメント時間と異なる場合、AWS Elemental MediaPackage は最も近いセグメント時間の倍数にセグメントを切り捨てます。
3. (オプション) [ライブプレイリストウィンドウの期間] に、親マニフェストの総時間 (秒単位) を入力します。
4. (オプション) すべてのオーディオトラックを 1 つの HLS レンディショングループにまとめるには、[オーディオレンディショングループを使用] を選択します。レンディショングループの詳細

については、「[AWS Elemental MediaPackage のレンディショングループのリファレンス](#)」を参照してください。

- (オプション) DVB の字幕を出力にパススルーするには、[DVB 字幕を含める] を選択します。
- (オプション) 他のトラックとともに追加の I フレームのみのストリームをマニフェストに含めるには、[IFrame のみのストリームを含める] を選択します。MediaPackage は、マニフェストの最初のレンディションから I フレーム専用ストリームを生成します。サービスは EXT-I-FRAMES-ONLY タグを出力マニフェストに挿入し、I フレーム専用再生リストを生成した上で、それをストリームに含めます。この再生リストでは、早送りや巻き戻しなどのプレイヤー機能を利用できません。
- (オプション) [プログラムの日付/時間間隔] に、MediaPackage によって EXT-X-PROGRAM-DATE-TIME タグがマニフェストに挿入される間隔 (秒単位) を入力します。

EXT-X-PROGRAM-DATE-TIME タグには、セグメントの時間が保持されます。ソースコンテンツでプログラム日時 (PDT) に関する情報が利用可能な場合、MediaPackage は、それと同じ情報を出力コンテンツにも使用します。それ以外の場合、MediaPackage は PDT に協定世界時 (UTC) を使用します。

PDT 情報は、ダウンストリームプレイヤーがストリームをウォールクロックに同期させるのに役立ちます。それにより、視聴者が再生タイムラインでシークしたり、プレイヤーで時間を表示したりするなどの機能が有効になります。

- (オプション) [プレイリストタイプ] で、[イベント] または [VOD] を選択します。イベントまたは VOD として指定すると、対応する EXT-X-PLAYLIST-TYPE エントリがメディアプレイリストに含まれます。プレイリストが live to VOD コンテンツであるかどうかを示します。

## SCTE-35 に関するオプション

以下の各フィールドにより、MediaPackage が入力ストリームからの SCTE-35 メッセージを、どのように処理するかを決定します。詳細については、「[AWS Elemental MediaPackage の SCTE-35 メッセージオプション](#)」を参照してください。

- (オプション) [広告マーカー] で、パッケージ化したコンテンツに広告マーカーを含める方法を選択します。

次から選択します。

- [None] (なし) – すべての SCTE-35 広告マーカーを出力から省きます。
- パススルー – SCTE-35 広告マーカーを、入力 HLS の入力ストリームから出力に直接コピーします。

- SCTE-35 Enhanced – 入カストリームの SCTE-35 入カメッセージに基づいて、出力で広告マーカとブラックアウトタグを生成します。
  - 日付範囲 – 広告やプログラムの移行を知らせるために HLS および CMAF マニフェストで EXT-X-DATERANGE タグを出力します。
2. (オプション) [広告トリガー] で、出力で広告マーカとして扱う SCTE-35 メッセージタイプを選択します。ここでの選択を行わない場合、MediaPackage は、以下のメッセージタイプに基づいた広告マーカを出力マニフェストに挿入します。
- スプライス挿入
  - プロバイダー広告
  - ディストリビューター広告
  - プロバイダー配置機会
  - ディストリビューター配置機会
3. (オプション) [配信制限に関する広告] で、SCTE-35 メッセージのセグメンテーション記述子内の配信制限フラグに基づいて MediaPackage が実行する広告挿入アクションを選択します。
- [None] (なし) – MediaPackage は、出力マニフェストに広告マーカを挿入しません。
  - [Restricted] (制限あり) – [Customize ad triggers] (広告トリガーをカスタマイズ) で指定した、SCTE-35 メッセージタイプでの配信制限がある場合に、MediaPackage は広告マーカを挿入します。
  - [Unrestricted] (制限なし) – [Customize ad triggers] (広告トリガーをカスタマイズ) で指定した、SCTE-35 メッセージタイプでの配信制限がない場合に、MediaPackage は広告マーカを挿入します。
  - [Both] (両方) – [Customize ad triggers] (広告トリガーをカスタマイズ) で指定した、SCTE-35 メッセージタイプでの配信制限があるかどうかにかかわらず、MediaPackage は広告マーカを挿入します。

## パッケージの暗号化フィールド

コンテンツ暗号化とデジタル著作権管理 (DRM) によって、コンテンツを不正使用から保護します。AWS Elemental MediaPackage は [AWS Secure Packager and Encoder Key Exchange \(SPEKE\) API](#) を使用して、DRM プロバイダーによるコンテンツの暗号化と復号化を容易にします。SPEKE を使用する DRM プロバイダーは、SPEKE API を通じて MediaPackage に暗号化キーを提供します。同時に DRM プロバイダーは、サポートしているメディアプレイヤー用に復号化のためのライセンスも提供します。クラウドで実行されているサービスや機能での SPEKE の使用について

は、Secure Packager and Encoder Key Exchange API Specification guide の「[AWS cloud-based architecture](#)」を参照してください。

**Note**

コンテンツを暗号化するには、DRM プロバイダーが必要で、暗号化を使用するように設定する必要があります。詳細については、[the section called “コンテンツの暗号化と DRM”](#)を参照してください。

暗号化の値を定義します。

1. 著作権保護なしでコンテンツを提供するには、[No encryption] (暗号化なし) を選択したままにします。
2. 著作権を保護してコンテンツを提供するには、[Encrypt content (コンテンツの暗号化)] を選択して追加のフィールドに以下のように入力します。
  - a. [Resource ID] (リソース ID) で、コンテンツの識別子を入力します。この ID は、現在のエンドポイントを特定するために、サービスよりキーサーバーに送信されます。この設定を、どの程度特有なものにするかは、どの程度詳細なアクセス制御を求めるかによって異なります。このサービスでは、同時に実行される 2 つの暗号化プロセスで、同じ ID を使用することはできません。リソース ID は、コンテンツ ID とも呼ばれます。

次に、リソース ID の例を示します。

```
MovieNight20171126093045
```

- b. [システム ID] に、ストリーミングプロトコルと DRM システムの一意の識別子を入力します。システム ID を 1 つ指定します。ID がわからない場合は、DRM プロバイダーにお問い合わせください。
- c. [URL] に、キーサーバーと通信するためにセットアップした API Gateway プロキシの URL を入力します。API Gateway プロキシは、MediaPackage と同じ AWS リージョンに置かれている必要があります。

次は、その URL の例です。

```
https://1wm2dx1f33.execute-api.us-west-2.amazonaws.com/SpekeSample/copyProtection
```



- d. [Role ARN] (ロール ARN) で、API Gateway を介してリクエストを送信するためのアクセス権限を付与する、IAM ロールの Amazon リソースネーム (ARN) を入力します。これは、DRM ソリューションプロバイダーから取得します。

以下は、ロール ARN の例です。

```
arn:aws:iam::444455556666:role/SpekeAccess
```

- e. [Certificate ARN] (証明書 ARN) – (オプション) コンテンツキーでの暗号化に使用する 2048 RSA 証明書 ARN を入力します。このオプションは、DRM キープロバイダーがコンテンツキーの暗号化をサポートしている場合にのみ使用してください。キープロバイダーがサポートしていない場合は、この暗号化を使用してもイベントが失敗します。

ここに証明書 ARN を入力するには、対応する証明書を AWS Certificate Manager に既にインポートしている必要があります。その上で ACM からの証明書 ARN をここに入力します。

コンテンツキーの暗号化については、「[コンテンツキーで使用する証明書の準備と管理](#)」を参照してください。

- f. [Encryption method] (暗号化方法) では、Apple HLS FairPlay に対しては [Sample-AES] を、Apple HLS AES-128 に対しては [AES-128] を、それぞれの場合に応じて選択します。
- g. (オプション) [Constant initialization vector] (定数初期化ベクトル) に、コンテンツを暗号化するためのキーで使用される、128 ビット (16 バイト) の 16 進値を、32 文字の文字列により入力します。
- h. (オプション) [Key rotation interval] (キーローテーションの間隔) に、コンテンツがリアルタイムでストリーミングされるライブワークフローでの、キーの変更頻度を秒単位で入力します。サービスは、ライブコンテンツのストリーミングを開始する前にコンテンツキーを取得します。その後は、必要に応じてワークフローの存続期間中にそれらを取得します。デフォルトでは、キーのローテーションは 60 秒間隔に設定されています (60 を設定するのと同じです)。キーのローテーションを無効にするには、この間隔を 0 (ゼロ) に設定します。

次の設定例では、サービスは 30 分ごとにキーのローテーションを実行します。

```
1800
```

キーローテーションについては、「[キーローテーションの動作について](#)」を参照してください。

- i. (オプション) マニフェストのすべてのセグメントの前に、サービスに同じキーを繰り返させたい場合は、[Repeat EXT-X-KEY] (EXT-X-KEY を繰り返す) を選択します。デフォルトでは、キーは、ヘッダーの後、セグメントの前に一度だけ書き込まれます。[Repeat EXT-X-KEY] (EXT-X-KEY を繰り返す) を選択すると、マニフェストはすべてのセグメントにキーが前置される形式で (ヘッダー、キー、セグメント、キー、セグメント、キー... のように) 記述されます。この設定は、プレイヤーの要件に合わせて行ってください。このオプションを選択すると、DRM サーバーへのクライアントリクエストが増える場合があります。

## アクセスコントロールの設定フィールド

アクセスコントロールの値を定義します。

1. このエンドポイントでリクエスト側デバイスにコンテンツを提供できるようにするには、[オリジンを許可する] を選択します。エンドポイントで配信を禁止することは一般的ではありません。

通常、エンドポイントでのコンテンツの提供を禁止するのは、エンドポイントがライブストリームからの VOD コンテンツの収集専用に使われている場合のみです。詳細については、「[AWS Elemental MediaPackage を使用した live-to-VOD アセットの作成](#)」を参照してください。

2. [すべての受信クライアントを許可する] を選択してすべてのリクエスト側 IP アドレスと IP 範囲にコンテンツを提供するか、[IP アドレスによる制限] を選択してこのエンドポイントが提供する IP アドレスを制限します。IP アドレスによって制限する場合は、[IP 許可リスト] に、このエンドポイントでコンテンツを提供する IP アドレスと IP 範囲を入力します。1 行に 1 つの CIDR ブロックです。

### Note

IPv4 アドレスのみが許可されます。

3. [CDN 認証の使用] を選択して、このエンドポイントへのコンテンツリクエストに有効な認証コードを含めなければならないようにします。残りのフィールドに入力します。
  - a. [シークレットロール ARN] に、MediaPackage に対して AWS Secrets Manager へのアクセス権限を付与する IAM ロールの ARN を入力します。シークレットロール ARN は次の形式である必要があります: `arn:aws:iam::accountID:role/name`
  - b. [CDN 識別子シークレット ARN] に、CDN がエンドポイントへのアクセス承認に使用する Secrets Manager での認証コードシークレットの ARN を入力します。CDN 識別子のシークレット ARN は次の形式である必要があります: `arn:aws:secretsmanager:region:accountID:secretguid`。



この認証の仕組みについては、「[AWS Elemental MediaPackage での CDN 認証](#)」を参照してください。

## ストリーム選択に関するフィールド

含めるストリームを定義します。

最小値と最大値で考慮されるのは、ビデオのビットレートのみです。動画ビットレートが指定した最小値未満の場合、他のトラックの総ビットレートに関係なく、その動画は出力に含まれません。同様に、ビデオのビットレートが、指定した最大値未満の場合、他のトラックの総ビットレートに関係なしに、ビデオは出力に含まれます。

1. (オプション) [Stream order] (ストリーム順) で、以下から選択します。
  - Original (オリジナル): 着信ソースと同じ順に従って出力ストリームをソートします。
  - 動画ビットレート昇順: 最小のビットレートから開始して最大のビットレートで終わるように出力ストリームをソートします。
  - 動画ビットレート降順: 最大のビットレートから開始して最小のビットレートで終わるように出力ストリームをソートします。
2. (オプション) [最小動画ビットレート] に、このエンドポイントから再生可能な動画トラックの要件とする最小ビットレート (1 秒あたりのビット数) を入力します。
3. (オプション) [最大動画ビットレート] に、このエンドポイントから再生可能な動画トラックの要件とする最大ビットレート (1 秒あたりのビット数) を入力します。

## DASH エンドポイントの作成

MPEG-DASH をサポートするデバイス向けにコンテンツをフォーマットするエンドポイントを作成します。

MPEG-DASH エンドポイントを作成するには (コンソール)

1. エンドポイントに関連付けるチャンネルにアクセスします。手順については、「[チャンネルの詳細の表示](#)」を参照してください。
2. チャンネルの詳細ページの [オリジンエンドポイント] で、[エンドポイントの管理] を選択します。
3. [Manage endpoints] (エンドポイント管理) を選択します。
4. 以下のトピックの説明に従ってフィールドに入力します。

- [エンドポイントでの新しいフィールド](#)
- [パッケージ設定のフィールド](#)
- [パッケージの暗号化フィールド](#)
- [アクセスコントロールの設定フィールド](#)
- [ストリーム選択に関するフィールド](#)

## 5. [Save (保存)] を選択します。

AWS Elemental MediaPackage コンソールからの Amazon CloudFront デイストリビューションの作成を有効化しており、チャンネルに初めてエンドポイントを作成した場合は、MediaPackage によって、このデイストリビューションにオリジンが追加されます。CloudFront での CDN の URL とエンドポイントの情報は、チャンネルの詳細ページにあるエンドポイントセクションで確認できます。

エンドポイントがアクティブになり、その URL のエンドポイントにリクエストが送信されると、すぐにコンテンツを配信できます。MediaPackage は、トラフィックに合わせて適切な容量が使用できるよう、リソースをスケールアップまたはスケールダウンします。

エンドポイントの作成時にアカウントのクォータを超過した場合は、エラーが発生します。この際のエラーは、「リクエストが多すぎます。もう一度お試しください。」といった内容です。「リソース上限の超過」とは、API リクエストのクォータを超過しているか、エンドポイントの数がチャンネルで使用できる上限に既に到達していることを意味しています。このエラーが誤って表示されたと思われる場合は、Service Quotas コンソールを使用して、[クォータの引き上げをリクエスト](#)してください。MediaPackage でのクォータの詳細については、「[AWS Elemental MediaPackage のクォータ](#)」を参照してください。

## エンドポイントでの新しいフィールド

エンドポイントの作成中に、[名前] フィールドのような自由記述のフィールドに顧客アカウント番号などの機密扱いの識別情報を入力しないようにしてください。これは、MediaPackage コンソール、MediaPackage API、AWS CLI、AWS SDK を使用して AWS Elemental MediaPackage を操作する場合も同様です。MediaPackage に入力するデータはすべて、取得され、診断ログもしくは Amazon CloudWatch Events に包含される場合があります。

1. [ID] に、エンドポイントの説明となるような名前を入力します。ID はエンドポイントのプライマリ識別子であり、AWS リージョン 内のアカウントに対して一意である必要があります。

2. (オプション) [説明] に、エンドポイントを特定する際に手掛かりとなる説明テキストを入力します。
3. [Manifest name] (マニフェスト名) に、エンドポイント URL の末尾に付加する短い文字列を入力します。マニフェスト名により、このエンドポイントへの一意のパスを作成できます。
4. (オプション) [スタートオーバーウィンドウ] に、ウィンドウのサイズ (秒単位) を入力して、オンデマンド表示に利用できるライブストリームのウィンドウを作成します。視聴者は、ウィンドウ範囲内のコンテンツのスタートオーバーまたはキャッチアップを行うことができます。スタートオーバーとキャッチアップ TV の実装の詳細については、「[AWS Elemental MediaPackage のタイムシフト表示のリファレンス](#)」を参照してください。
5. (オプション) [時間遅延] に、遅延時間 (秒単位) を入力して、プレイヤーでコンテンツを利用できるようになる時間を遅らせます。最小の設定時間は 5 秒間です。最大時間は 86,400 秒 (24 時間) です。

時間遅延を使用してライブポイントを再定義し、「現在」の時刻から指定した遅延を差し引いた時刻にコンテンツを利用可能にします。例えば、時間遅延を 60 秒に設定している場合、MediaPackage が 12:20 に受信したコンテンツは 12:21 まで利用できません。12:20 の再生リクエストに対しては、12:19 のコンテンツが提供されます。同様に、タイムゾーンをまたいで提供するコンテンツの場合、タイムゾーンの時差に等しい時間遅延を設定することで、たとえば現地時間の 8:00 にコンテンツを提供できます。

遅延時間とスタートオーバーウィンドウを併用する場合は、時間遅延をスタートオーバーウィンドウより短くする必要があります。

#### Tip

短い出力セグメントで入力の冗長性を利用している場合は、時間遅延を使用することで、入力スイッチング時のバッファリング量を低減できます。遅延により、コンテンツ再生時のレイテンシーが増加する可能性があることに注意してください。

## パッケージ設定のフィールド

1. [パッケージタイプ] で、[DASH-ISO] を選択します。
2. (オプション) [Segment duration (セグメント時間)] に、各セグメントの時間 (秒単位) を入力します。入力セグメントの長さと同じか、その倍数の値を入力します。入力した値が入力セグメント時間と異なる場合、AWS Elemental MediaPackage は最も近いセグメント時間の倍数にセグメントを切り捨てます。

**⚠ Important**

[Segment template format] (セグメントテンプレートの形式)で [Number with duration] (期間を含む数値) を有効化した場合、エンドポイントの作成後はセグメント期間を変更することはできません。


3. (オプション) [マニフェストウィンドウ所要時間] に、マニフェストの総時間 (秒単位) を入力します。
4. (オプション) [プロファイル]で、出力のセグメント形式とマニフェスト形式を決定する DASH プロファイルを選択します。
  - なし – 出力で DASH プロファイルを使用しません。
  - Hbbtv 1.5 – 出力は HbbTV v1.5 に準拠します。HbbTV v1.5 の詳細については、[HbbTV の仕様に関するウェブサイト](#)を参照してください。
  - Hybridcast — 出力は Hybridcast に準拠します。Hybridcast の詳細については、[IPTV Forum Japan の Hybridcast の仕様](#)を参照してください。パッケージ設定で Hybridcast プロファイルを有効にすると、DASH の [期間トリガー] は使用できません。
  - DVB-DASH 2014 - 出力は DVB-DASH 2014 に準拠します。DVB-DASH 2014 の詳細については、[DVB-DASH の仕様](#)を参照してください。
5. (オプション) [マニフェストのレイアウト] で、MediaPackage が再生リクエストに対応して、完全なマニフェストを提供するか、圧縮されたマニフェストを提供するかを指定します。
  - [Full] (完全) を選択した場合、MediaPackage はマニフェストのすべての Representation について、SegmentTemplate および SegmentTimeline タグを記述します。
  - [Compact] (圧縮) を選択した場合、MediaPackage は重複した SegmentTemplate タグを統合し、マニフェストの先頭に記述します。これによりマニフェストが短くなり、一部のデバイスで処理が容易になります。

マニフェストのレイアウトオプションの詳細については、「[圧縮された DASH マニフェスト](#)」を参照してください。

6. (オプション) [最小更新期間] に、プレイヤーがマニフェストの更新をリクエストする前に待機する最小時間 (秒単位) を入力します。値が小さいほど、マニフェストの更新回数が増えます。ただし、リクエストとレスポンスのネットワークトラフィックも増えます。
7. (オプション) [Min buffer time (最小バッファ時間)] に、プレイヤーがバッファに保持する必要がある最小時間 (秒単位) を入力します。ネットワーク条件のせいで再生が中断する場合は、再生が失

敗する前に追加のコンテンツがプレイヤーにバッファされ、視聴者に影響が及ばないように復旧時間が確保されます。

8. (オプション) [Suggested presentation delay] (推奨表示遅延) に、マニフェストの末尾からプレイヤーを戻す時間 (秒単位) を入力します。これにより、コンテンツの開始ポイントがマニフェストの末尾から x 秒戻った (コンテンツがライブである) ポイントに設定されます。たとえば、表示遅延を 35 秒に設定すると、5:30 のリクエストに対して 5:29:25 からのコンテンツが提供されます。時間遅延を使用すると、MediaPackage は時間遅延に推奨された表示遅延を追加します。
9. (オプション) [セグメントテンプレート形式] で、各セグメントが MediaPackage および再生リクエストからどのように参照されるかを選択します。
  - [Number with timeline] (タイムライン付き番号) を選択した場合、MediaPackage は \$Number\$ 変数を使用して、SegmentTemplate タグの media 属性のセグメントを参照します。変数の値はセグメントの連続番号です。SegmentTimeline は各セグメントテンプレートに含まれています。
  - [Number with duration] (期間付き番号) を選択すると、MediaPackage は \$Number\$ 変数を使用して、SegmentTimeline オブジェクトをセグメントテンプレートの duration 属性と置き換えます。

 Note

このオプションは、複数期間 DASH と組み合わせて使用することはできません。

- [Time with timeline] (タイムライン付き時間) を選択した場合、MediaPackage はセグメントを参照するために \$Time\$ 変数を使用します。変数の値は、マニフェストタイムライン上でセグメントが開始されるときタイムスタンプです。SegmentTimeline は各セグメントテンプレートに含まれています。

SegmentTemplate タグの書式設定オプションの詳細については、「[DASH マニフェストのセグメントテンプレート形式](#)」を参照してください。

- 10(オプション) [UTC タイミング] で、プレイヤーを協定世界時 (UTC) での実測時間に同期するために使用する方法を選択します。これにより、プレイヤーと MediaPackage が、UTC での同じ実測時間で実行するようになります。この同期は必須で、これを行わないと再生のタイミングや同期に問題が発生する可能性があります。

使用できるオプションは HTTP-HEAD、HTTP-ISO、HTTP-XSDATE、NONE です。この値は、アウトバウンド向け MPD (Media Presentation Description) の UTCTiming 要素に、@schemeIdURI 属性としてセットされます。UTCTiming については、[DASH](#) の UTC タイミング記述子、5.8.4.11 を参照してください。

- 11(オプション) [UTC タイミング URI] で、UTC との同期に使用する URI を指定します。この URI は、[UTC timing] (UTC タイミング) で定義されたスキームに従って、タイミングデータをフェッチする際に使用されます。この値は、[UTC timing] (UTC タイミング) が NONE に設定されていない場合にのみ有効となります。この値は、UTCTiming 要素に @value 属性としてセットされます。@value の詳細については、[DASH](#) の、DASH UTC Timing Schemes、5.8.5.7 を参照してください。
- 12(オプション) 他のトラックとともに追加の I フレームのみのストリームをマニフェストに含めるには、[IFrame のみのストリームを含める] を選択します。MediaPackage は、マニフェストの最初のレンディションから I フレーム専用ストリームを生成します。このサービスは、<EssentialProperty schemeIdUri="http://dashif.org/guidelines/trickmode" value="X"/> の記述子 (X は元の適応セットの ID) を挿入し、I フレームのみのレンディションを生成してそれをストリームに含めます。暗号化を使用する場合、MediaPackage は I フレームのみのレンディションを元の動画レンディションと同じコンテンツキーで暗号化します。このレンディションでは、早送りや巻き戻しなどのプレイヤー機能を利用できます。
- 13[期間トリガー] で、MediaPackage が DASH 出カマニフェストでメディアプレゼンテーション説明 (MPD) の期間を作成する方法を選択します。次から選択します。
- [None] (なし) – MediaPackage は追加の期間を作成しません。マニフェストを 1 つの期間としてフォーマットし、このセグメントには SCTE-35 マーカーを含みません。
  - [Trigger new periods on ads] (広告の新しい期間をトリガーする) – MediaPackage は入力コンテンツの SCTE-35 広告マーカーに基づいて、マニフェストに複数期間を作成して挿入します。これらの期間は、メインコンテンツと広告コンテンツの間の境界コンテンツのように、コンテンツを分割します。MediaPackage によるマニフェスト内での期間設定の詳細については、「[AWS Elemental MediaPackage の DASH マニフェストオプション](#)」を参照してください。

#### Important

複数期間は、DASH コンテンツで広告挿入をパーソナライズするために AWS Elemental MediaTailor を使用する場合に必要です。このサービスの詳細については、[AWS Elemental MediaTailor ユーザーガイド](#)を参照してください。

## SCTE-35 に関するオプション

以下の各フィールドにより、MediaPackage が入カストリームからの SCTE-35 メッセージを、どのように処理するかを決定します。詳細については、「[AWS Elemental MediaPackage の SCTE-35 メッセージオプション](#)」を参照してください。



1. (オプション) [広告トリガー] で、出力で広告マーカースとして扱う SCTE-35 メッセージタイプを選択します。ここでの選択を行わない場合、MediaPackage は、以下のメッセージタイプに基づいた広告マーカースを出力マニフェストに挿入します。
  - スプライス挿入
  - プロバイダー広告
  - ディストリビューター広告
  - プロバイダー配置機会
  - ディストリビューター配置機会
2. (オプション) [配信制限に関する広告] で、SCTE-35 メッセージのセグメンテーション記述子内の配信制限フラグに基づいて MediaPackage が実行する広告挿入アクションを選択します。
  - [None] (なし) – MediaPackage は、出力マニフェストに広告マーカースを挿入しません。
  - [Restricted] (制限あり) – [Customize ad triggers] (広告トリガーをカスタマイズ) で指定した、SCTE-35 メッセージタイプでの配信制限がある場合に、MediaPackage は広告マーカースを挿入します。
  - [Unrestricted] (制限なし) – [Customize ad triggers] (広告トリガーをカスタマイズ) で指定した、SCTE-35 メッセージタイプでの配信制限がない場合に、MediaPackage は広告マーカースを挿入します。
  - [Both] (両方) – [Customize ad triggers] (広告トリガーをカスタマイズ) で指定した、SCTE-35 メッセージタイプでの配信制限があるかどうかにかかわらず、MediaPackage は広告マーカースを挿入します。

広告マーカースを挿入しないことを選択すると、MediaPackage も期間を生成しません。出力マニフェストは 1 つの期間に含まれています。

## パッケージの暗号化フィールド

コンテンツ暗号化とデジタル著作権管理 (DRM) によって、コンテンツを不正使用から保護します。AWS Elemental MediaPackage は [AWS Secure Packager and Encoder Key Exchange \(SPEKE\) API](#) を使用して、DRM プロバイダーによるコンテンツの暗号化と復号化を容易にします。SPEKE を使用する DRM プロバイダーは、SPEKE API を通じて MediaPackage に暗号化キーを提供します。同時に DRM プロバイダーは、サポートしているメディアプレイヤー用に復号化のためのライセンスも提供します。クラウドで実行されているサービスや機能での SPEKE の使用については、Secure Packager and Encoder Key Exchange API Specification guide の「[AWS cloud-based architecture](#)」を参照してください。

**Note**

コンテンツを暗号化するには、DRM ソリューションプロバイダーが必要で、暗号化を使用するように設定する必要があります。詳細については、[the section called “コンテンツの暗号化と DRM”](#)を参照してください。

暗号化の値を定義します。

1. 著作権保護なしでコンテンツを提供するには、[No encryption] (暗号化なし) を選択したままにします。
2. 著作権を保護してコンテンツを提供するには、[Encrypt content (コンテンツの暗号化)] を選択して追加のフィールドに以下のように入力します。
  - a. [Resource ID] (リソース ID) で、コンテンツの識別子を入力します。この ID は、現在のエンドポイントを特定するために、サービスよりキーサーバーに送信されます。この設定を、どの程度特有用なものにするかは、どの程度詳細なアクセス制御を求めるかによって異なります。このサービスでは、同時に実行される 2 つの暗号化プロセスで、同じ ID を使用することはできません。リソース ID は、コンテンツ ID とも呼ばれます。

以下に、リソース ID の例を示します。

```
MovieNight20171126093045
```

- b. [System IDs] (システム ID) に、ストリーミングプロトコルと DRM システムの一意の識別子を入力します。最大 2 つの ID を指定します。複数のシステム ID を指定する場合は、1 行に 1 つずつ入力して、[Add] (追加) をクリックします。一般的なシステム ID のリストについては、「[DASH-IF システム ID](#)」を参照してください。ID がわからない場合は、DRM ソリューションプロバイダーにお問い合わせください。
- c. [URL] に、キーサーバーと通信するためにセットアップした API Gateway プロキシの URL を入力します。API Gateway プロキシは、MediaPackage と同じ AWS リージョン に置かれている必要があります。

次は、その URL の例です。

```
https://1wm2dx1f33.execute-api.us-west-2.amazonaws.com/SpekeSample/copyProtection
```



- d. [Role ARN] (ロール ARN) で、API Gateway を介してリクエストを送信するためのアクセス権限を付与する、IAM ロールの Amazon リソースネーム (ARN) を入力します。これは、DRM ソリューションプロバイダーから取得します。

以下は、ロール ARN の例です。

```
arn:aws:iam::444455556666:role/SpekeAccess
```

- e. (オプション) [SPEKE バージョン] で、暗号化に使用する SPEKE のバージョンを選択します。SPEKE バージョン 1.0 は CPIX バージョン 2.0 を使用するレガシーバージョンであり、単一キーによる暗号化をサポートしています。SPEKE バージョン 2.0 では CPIX バージョン 2.3 が使用されており、複数のキーによる暗号化がサポートされます。MediaPackage で SPEKE を使用方法の詳細については、「[AWS Elemental MediaPackage でのコンテンツの暗号化と DRM](#)」を参照してください。

[SPEKE Version 2.0] (SPEKE バージョン 2.0) を選択した場合には、[Video encryption preset] (ビデオ暗号化プリセット) と [Audio encryption preset] (オーディオ暗号化プリセット) も選択します。このビデオおよびオーディオのプリセット設定により、MediaPackage がストリーム内のビデオとオーディオのトラックを暗号化する際に使用する、コンテンツキーが決定します。これらのプリセットの詳細については、「[SPEKE バージョン 2.0 のプリセット](#)」を参照してください。

SPEKE バージョン 2.0 を使用する場合、MediaPackage ではキーのローテーションが無効化されます。

- f. [Certificate ARN] (証明書 ARN) – (オプション) コンテンツキーでの暗号化に使用する 2048 RSA 証明書 ARN を入力します。このオプションは、DRM キープロバイダーがコンテンツキーの暗号化をサポートしている場合にのみ使用してください。キープロバイダーがサポートしていない場合は、この暗号化を使用してもイベントが失敗します。

ここに証明書 ARN を入力するには、対応する証明書を AWS Certificate Manager に既にインポートする必要があります。その上で ACM からの証明書 ARN をここに入力します。

コンテンツキーの暗号化については、「[コンテンツキーで使用する証明書の準備と管理](#)」を参照してください。

- g. (オプション) [Key rotation interval] (キーローテーションの間隔) に、コンテンツがリアルタイムでストリーミングされるライブワークフローでの、キーの変更頻度を秒単位で入力します。サービスは、ライブコンテンツのストリーミングを開始する前にコンテンツキーを取得します。その後は、必要に応じてワークフローの存続期間中にそれらを取得します。デフォルトで

は、キーのローテーションは 60 秒間隔に設定されています (60 を設定するのと同じです)。キーのローテーションを無効にするには、この間隔を 0 (ゼロ) に設定します。

次の設定例では、サービスは 30 分ごとにキーのローテーションを実行します。

1800

キーローテーションについては、「[キーローテーションの動作について](#)」を参照してください。

## アクセスコントロールの設定フィールド

アクセスコントロールの値を定義します。

1. このエンドポイントでリクエスト側デバイスにコンテンツを提供できるようにするには、[オリジンを許可する] を選択します。エンドポイントで配信を禁止することは一般的ではありません。

通常、エンドポイントでのコンテンツの提供を禁止するのは、エンドポイントがライブストリームからの VOD コンテンツの収集専用に使われている場合のみです。詳細については、「[AWS Elemental MediaPackage を使用した live-to-VOD アセットの作成](#)」を参照してください。

2. [すべての受信クライアントを許可する] を選択してすべてのリクエスト側 IP アドレスと IP 範囲にコンテンツを提供するか、[IP アドレスによる制限] を選択してこのエンドポイントが提供する IP アドレスを制限します。IP アドレスによって制限する場合は、[IP 許可リスト] に、このエンドポイントでコンテンツを提供する IP アドレスと IP 範囲を入力します。1 行に 1 つの CIDR ブロックです。
3. [CDN 認証の使用] を選択して、このエンドポイントへのコンテンツリクエストに有効な認証コードを含めなければならないようにします。
4. (オプション) [シークレットロール ARN] に、MediaPackage に対して AWS Secrets Manager へのアクセス権限を付与する IAM ロールの ARN を入力します。シークレットロール ARN は次の形式である必要があります: `arn:aws:iam::accountID:role/name`。
5. (オプション) [CDN 識別子シークレット ARN] に、CDN がエンドポイントへのアクセス承認に使用する Secrets Manager での認証コードシークレットの ARN を入力します。CDN 識別子は次の形式である必要があります: `arn:aws:secretsmanager:region:accountID:secret:guid`。

この認証の仕組みについては、「[AWS Elemental MediaPackage での CDN 認証](#)」を参照してください。

## ストリーム選択に関するフィールド

含めるストリームを定義します。

最小値と最大値で考慮されるのは、ビデオのビットレートのみです。動画ビットレートが指定した最小値未満の場合、他のトラックの総ビットレートに関係なく、その動画は出力に含まれません。同様に、ビデオのビットレートが、指定した最大値未満の場合、他のトラックの総ビットレートに関係なしに、ビデオは出力に含まれます。

1. (オプション) [ストリームの順序] で、プレイヤーに表示される動画ビットレートの順序を選択します。
  - Original (オリジナル): 着信ソースと同じ順に従って出力ストリームをソートします。
  - 動画ビットレート昇順: 最小のビットレートから開始して最大のビットレートで終わるように出力ストリームをソートします。
  - 動画ビットレート降順: 最大のビットレートから開始して最小のビットレートで終わるように出力ストリームをソートします。
2. (オプション) [最小動画ビットレート] に、このエンドポイントから再生可能な動画トラックの要件とする最小ビットレート (1 秒あたりのビット数) を入力します。
3. (オプション) [最大動画ビットレート] に、このエンドポイントから再生可能な動画トラックの要件とする最大ビットレート (1 秒あたりのビット数) を入力します。

## Microsoft Smooth Streaming エンドポイントの作成

Microsoft Smooth Streaming をサポートするデバイス向けにコンテンツをフォーマットするエンドポイントを作成します。

Microsoft Smooth Streaming エンドポイントを作成するには (コンソール)

1. エンドポイントに関連付けるチャンネルにアクセスします。手順については、「[チャンネルの詳細の表示](#)」を参照してください。
2. チャンネルの詳細ページの [オリジンエンドポイント] で、[エンドポイントの管理] を選択します。
3. 以下のトピックの説明に従ってフィールドに入力します。
  - [エンドポイントでの新しいフィールド](#)
  - [パッケージ設定のフィールド](#)

- [パッケージの暗号化フィールド](#)
- [アクセスコントロールの設定フィールド](#)
- [ストリーム選択に関するフィールド](#)

#### 4. [Save (保存)] を選択します。

AWS Elemental MediaPackage コンソールからの Amazon CloudFront デイストリビューションの作成を有効化しており、チャンネルに初めてエンドポイントを作成した場合は、MediaPackage によって、このデイストリビューションにオリジンが追加されます。CloudFront での CDN の URL とエンドポイントの情報は、チャンネルの詳細ページにあるエンドポイントセクションで確認できます。

エンドポイントがアクティブになり、その URL のエンドポイントにリクエストが送信されると、すぐにコンテンツを配信できます。MediaPackage は、トラフィックに合わせて適切な容量が使用できるよう、リソースをスケールアップまたはスケールダウンします。

エンドポイントの作成時にアカウントのクォータを超過した場合は、エラーが発生します。この際のエラーは、「リクエストが多すぎます。もう一度お試しください。」といった内容です。「リソース上限の超過」とは、API リクエストのクォータを超過しているか、エンドポイントの数がチャンネルで使用できる上限に既に到達していることを意味しています。このエラーが誤って表示されたと思われる場合は、Service Quotas コンソールを使用して、[クォータの引き上げをリクエスト](#)してください。MediaPackage でのクォータの詳細については、「[AWS Elemental MediaPackage のクォータ](#)」を参照してください。

### エンドポイントでの新しいフィールド

エンドポイントの作成中に、[名前] フィールドのような自由記述のフィールドに顧客アカウント番号などの機密扱いの識別情報を入力しないようにしてください。これは、MediaPackage コンソール、MediaPackage API、AWS CLI、AWS SDK を使用して AWS Elemental MediaPackage を操作する場合も同様です。MediaPackage に入力するデータはすべて、取得され、診断ログもしくは Amazon CloudWatch Events に包含される場合があります。

1. [ID] に、エンドポイントの説明となるような名前を入力します。ID はエンドポイントのプライマリ識別子であり、AWS リージョン 内のアカウントに対して一意である必要があります。
2. (オプション) [説明] に、エンドポイントを特定する際に手掛かりとなる説明テキストを入力します。
3. [Manifest name] (マニフェスト名) に、エンドポイント URL の末尾に付加する短い文字列を入力します。マニフェスト名により、このエンドポイントへの一意のパスを作成できます。

4. (オプション) [スタートオーバーウィンドウ] に、ウィンドウのサイズ (秒単位) を入力して、オンデマンド表示に利用できるライブストリームのウィンドウを作成します。視聴者は、ウィンドウ範囲内のコンテンツのスタートオーバーまたはキャッチアップを行うことができます。スタートオーバーとキャッチアップ TV の実装の詳細については、「[AWS Elemental MediaPackage のタイムシフト表示のリファレンス](#)」を参照してください。
5. (オプション) [時間遅延] に、遅延時間 (秒単位) を入力して、プレーヤーでコンテンツを利用できるようになる時間を遅らせます。最小の設定時間は 5 秒間です。最大時間は 86,400 秒 (24 時間) です。

時間遅延を使用してライブポイントを再定義し、「現在」の時刻から指定した遅延を差し引いた時刻にコンテンツを利用可能にします。例えば、時間遅延を 60 秒に設定している場合、MediaPackage が 12:20 に受信したコンテンツは 12:21 まで利用できません。12:20 の再生リクエストに対しては、12:19 のコンテンツが提供されます。同様に、タイムゾーンをまたいで提供するコンテンツの場合、タイムゾーンの時差に等しい時間遅延を設定することで、たとえば現地時間の 8:00 にコンテンツを提供できます。

遅延時間とスタートオーバーウィンドウを併用する場合は、時間遅延をスタートオーバーウィンドウより短くする必要があります。

#### Tip

短い出力セグメントで入力の冗長性を利用している場合は、時間遅延を使用することで、入力スイッチング時のバッファリング量を低減できます。遅延により、コンテンツ再生時のレイテンシーが増加する可能性があることに注意してください。

## パッケージ設定のフィールド

パッケージ設定のフィールドには、エンドポイントに関する一般的な情報を保持します。

1. [パッケージタイプ] で、[Microsoft Smooth] を選択します。
2. (オプション) [Segment duration (セグメント時間)] に、各セグメントの時間 (秒単位) を入力します。入力セグメントの長さと同じか、その倍数の値を入力します。入力した値が入力セグメント時間と異なる場合、AWS Elemental MediaPackage は最も近いセグメント時間の倍数にセグメントを切り捨てます。
3. (オプション) [マニフェストウィンドウ所要時間] に、マニフェストの総時間 (秒単位) を入力します。

## パッケージの暗号化フィールド

コンテンツ暗号化とデジタル著作権管理 (DRM) によって、コンテンツを不正使用から保護します。AWS Elemental MediaPackage は [AWS Secure Packager and Encoder Key Exchange \(SPEKE\) API](#) を使用して、DRM プロバイダーによるコンテンツの暗号化と復号化を容易にします。SPEKE を使用する DRM プロバイダーは、SPEKE API を通じて MediaPackage に暗号化キーを提供します。同時に DRM プロバイダーは、サポートしているメディアプレイヤー用に復号化のためのライセンスも提供します。クラウドで実行されているサービスや機能での SPEKE の使用については、Secure Packager and Encoder Key Exchange API Specification guide の「[AWS cloud-based architecture](#)」を参照してください。

### Note

コンテンツを暗号化するには、DRM ソリューションプロバイダーが必要で、暗号化を使用するように設定する必要があります。詳細については、[the section called “コンテンツの暗号化と DRM”](#)を参照してください。

暗号化の値を定義します。

1. 著作権保護なしでコンテンツを提供するには、[No encryption] (暗号化なし) を選択したままにします。
2. 著作権を保護してコンテンツを提供するには、[Encrypt content (コンテンツの暗号化)] を選択して追加のフィールドに以下のように入力します。
  - a. [Resource ID] (リソース ID) で、コンテンツの識別子を入力します。この ID は、現在のエンドポイントを特定するために、サービスよりキーサーバーに送信されます。この設定を、どの程度特有なものにするかは、どの程度詳細なアクセス制御を求めるかによって異なります。このサービスでは、同時に実行される 2 つの暗号化プロセスで、同じ ID を使用することはできません。リソース ID は、コンテンツ ID とも呼ばれます。

次に、リソース ID の例を示します。

```
MovieNight20171126093045
```

- b. [システム ID] に、ストリーミングプロトコルと DRM システムの一意的識別子を入力します。1 つのシステム ID のみを指定します。ID がわからない場合は、DRM ソリューションプロバイダーにお問い合わせください。



- c. [URL] に、キーサーバーと通信するためにセットアップした API Gateway プロキシの URL を入力します。API Gateway プロキシは、MediaPackage と同じ AWS リージョンに置かれている必要があります。

次は、その URL の例です。

```
https://1wm2dx1f33.execute-api.us-west-2.amazonaws.com/SpekeSample/copyProtection
```

- d. [Role ARN] (ロール ARN) で、API Gateway を介してリクエストを送信するためのアクセス権限を付与する、IAM ロールの Amazon リソースネーム (ARN) を入力します。これは、DRM ソリューションプロバイダーから取得します。

以下は、ロール ARN の例です。

```
arn:aws:iam::444455556666:role/SpekeAccess
```

- e. [Certificate ARN] (証明書 ARN) – (オプション) コンテンツキーでの暗号化に使用する 2048 RSA 証明書 ARN を入力します。このオプションは、DRM キープロバイダーがコンテンツキーの暗号化をサポートしている場合にのみ使用してください。キープロバイダーがサポートしていない場合は、この暗号化を使用してもイベントが失敗します。

ここに証明書 ARN を入力するには、対応する証明書を AWS Certificate Manager に既にインポートしている必要があります。その上で ACM からの証明書 ARN をここに入力します。

キー暗号化については、「[コンテンツキーで使用する証明書の準備と管理](#)」を参照してください。

## アクセスコントロールの設定フィールド

アクセスコントロールの値を定義します。

1. このエンドポイントでリクエスト側デバイスにコンテンツを提供できるようにするには、[オリジンを許可する] を選択します。エンドポイントで配信を禁止することは一般的ではありません。

通常、エンドポイントでのコンテンツの提供を禁止するのは、エンドポイントがライブストリームからの VOD コンテンツの収集専用に使われている場合のみです。詳細については、「[AWS Elemental MediaPackage を使用した live-to-VOD アセットの作成](#)」を参照してください。

2. [すべての受信クライアントを許可する] を選択してすべてのリクエスト側 IP アドレスと IP 範囲にコンテンツを提供するか、[IP アドレスによる制限] を選択してこのエンドポイントが提供する

IP アドレスを制限します。IP アドレスによって制限する場合は、[IP 許可リスト] に、このエンドポイントでコンテンツを提供する IP アドレスと IP 範囲を入力します。1 行に 1 つの CIDR ブロックです。

3. [CDN 認証の使用] を選択して、このエンドポイントへのコンテンツリクエストに有効な認証コードを含めなければならないようにします。
4. (オプション) [シークレットロール ARN] に、MediaPackage に対して AWS Secrets Manager へのアクセス権限を付与する IAM ロールの ARN を入力します。シークレットロール ARN は次の形式である必要があります: `arn:aws:iam::accountID:role/name`。
5. (オプション) [CDN 識別子シークレット ARN] に、CDN がエンドポイントへのアクセス承認に使用する Secrets Manager での認証コードシークレットの ARN を入力します。CDN 識別子は次の形式である必要があります: `arn:aws:secretsmanager:region:accountID:secretguid`。

この認証の仕組みについては、「[AWS Elemental MediaPackage での CDN 認証](#)」を参照してください。

## ストリーム選択に関するフィールド

含めるストリームを定義します。

最小値と最大値で考慮されるのは、ビデオのビットレートのみです。動画ビットレートが指定した最小値未満の場合、他のトラックの総ビットレートに関係なく、その動画は出力に含まれません。同様に、ビデオのビットレートが、指定した最大値未満の場合、他のトラックの総ビットレートに関係なしに、ビデオは出力に含まれます。

1. (オプション) [ストリームの順序] で、プレイヤーに表示される動画ビットレートの順序を選択します。
  - Original (オリジナル): 着信ソースと同じ順に従って出カストリームをソートします。
  - 動画ビットレート昇順: 最小のビットレートから開始して最大のビットレートで終わるように出カストリームをソートします。
  - 動画ビットレート降順: 最大のビットレートから開始して最小のビットレートで終わるように出カストリームをソートします。
2. (オプション) [最小動画ビットレート] に、このエンドポイントから再生可能な動画トラックの要件とする最小ビットレート (1 秒あたりのビット数) を入力します。
3. (オプション) [最大動画ビットレート] に、このエンドポイントから再生可能な動画トラックの要件とする最大ビットレート (1 秒あたりのビット数) を入力します。



## CMAF エンドポイントの作成

Apple HLS fragmented MP4 (fMP4) をサポートするデバイス向けにコンテンツをフォーマットするエンドポイントを作成します。

CMAF エンドポイントを作成するには (コンソール)

1. エンドポイントに関連付けるチャンネルにアクセスします。手順については、「[チャンネルの詳細の表示](#)」を参照してください。
2. チャンネルの詳細ページの [オリジンエンドポイント] で、[エンドポイントの管理] を選択します。
3. 以下のトピックの説明に従ってフィールドに入力します。
  - [エンドポイントでの新しいフィールド](#)
  - [パッケージ設定のフィールド](#)
  - [パッケージの暗号化フィールド](#)
  - [アクセスコントロールの設定フィールド](#)
  - [ストリーム選択に関するフィールド](#)
4. [Save (保存)] を選択します。

AWS Elemental MediaPackage コンソールからの Amazon CloudFront デистриビューションの作成を有効化しており、チャンネルに初めてエンドポイントを作成した場合は、MediaPackage によって、このデистриビューションにオリジンが追加されます。CloudFront での CDN の URL とエンドポイントの情報は、チャンネルの詳細ページにあるエンドポイントセクションで確認できます。

エンドポイントがアクティブになり、その URL のエンドポイントにリクエストが送信されると、すぐにコンテンツを配信できます。MediaPackage は、トラフィックに合わせて適切な容量が使用できるよう、リソースをスケールアップまたはスケールダウンします。

エンドポイントの作成時にアカウントのクォータを超過した場合は、エラーが発生します。この際のエラーは、「リクエストが多すぎます。もう一度お試しください。」といった内容です。「リソース上限の超過」とは、API リクエストのクォータを超過しているか、エンドポイントの数がチャンネルで使用できる上限に既に到達していることを意味しています。このエラーが誤って表示されたと思われる場合は、Service Quotas コンソールを使用して、[クォータの引き上げをリクエスト](#)してください。MediaPackage でのクォータの詳細については、「[AWS Elemental MediaPackage のクォータ](#)」を参照してください。

## エンドポイントでの新しいフィールド

エンドポイントの作成中に、[名前] フィールドのような自由記述のフィールドに顧客アカウント番号などの機密扱いの識別情報を入力しないようにしてください。これは、MediaPackage コンソール、MediaPackage API、AWS CLI、AWS SDK を使用して AWS Elemental MediaPackage を操作する場合も同様です。MediaPackage に入力するデータはすべて、取得され、診断ログもしくは Amazon CloudWatch Events に包含される場合があります。

1. [ID] に、エンドポイントの説明となるような名前を入力します。ID はエンドポイントのプライマリ識別子であり、AWS リージョン 内のアカウントに対して一意である必要があります。
2. (オプション) [説明] に、エンドポイントを特定する際に手掛かりとなる説明テキストを入力します。
3. [Manifest name] (マニフェスト名) に、エンドポイント URL の末尾に付加する短い文字列を入力します。マニフェスト名により、このエンドポイントへの一意のパスを作成できます。
4. (オプション) [スタートオーバーウィンドウ] に、ウィンドウのサイズ (秒単位) を入力して、オンデマンド表示に利用できるライブストリームのウィンドウを作成します。視聴者は、ウィンドウ範囲内のコンテンツのスタートオーバーまたはキャッチアップを行うことができます。スタートオーバーとキャッチアップ TV の実装の詳細については、「[AWS Elemental MediaPackage のタイムシフト表示のリファレンス](#)」を参照してください。
5. (オプション) [時間遅延] に、遅延時間 (秒単位) を入力して、プレイヤーでコンテンツを利用できるようになる時間を遅らせます。最小の設定時間は 5 秒間です。最大時間は 86,400 秒 (24 時間) です。

時間遅延を使用してライブポイントを再定義し、「現在」の時刻から指定した遅延を差し引いた時刻にコンテンツを利用可能にします。例えば、時間遅延を 60 秒に設定している場合、MediaPackage が 12:20 に受信したコンテンツは 12:21 まで利用できません。12:20 の再生リクエストに対しては、12:19 のコンテンツが提供されます。同様に、タイムゾーンをまたいで提供するコンテンツの場合、タイムゾーンの時差に等しい時間遅延を設定することで、たとえば現地時間の 8:00 にコンテンツを提供できます。

遅延時間とスタートオーバーウィンドウを併用する場合は、時間遅延をスタートオーバーウィンドウより短くする必要があります。

**i** Tip

短い出力セグメントで入力の冗長性を利用している場合は、時間遅延を使用することで、入力スイッチング時のバッファリング量を低減できます。遅延により、コンテンツ再生時のレイテンシーが増加する可能性があることに注意してください。

## パッケージ設定のフィールド

パッケージ設定のフィールドには、エンドポイントに関する一般的な情報を保持します。

1. [パッケージタイプ] で、[Common Media Application Format (CMAF)] を選択します。
2. [HLS マニフェスト ID] に、マニフェストのプライマリ識別子となる ID を入力します。ID は、このエンドポイントに対して一意である必要があります。この ID は作成後には変更できません。
3. (オプション) [セグメントプレフィックス] に、HLS 子マニフェストのセグメントのカスタム名を入力します。このセグメントプレフィックスはセグメント名の先頭に追加され、セグメントごとに一意の識別子を作成します。

### Example

セグメントプレフィックスが `movie` である場合、子マニフェストからのセグメントは `movie_1_2.ts` になります。

4. (オプション) [Segment duration (セグメント時間)] に、各セグメントの時間 (秒単位) を入力します。入力セグメントの長さと同じか、その倍数の値を入力します。入力した値が入力セグメント時間と異なる場合、AWS Elemental MediaPackage は最も近いセグメント時間の倍数にセグメントを切り捨てます。
5. (オプション) [ライブプレイリストウィンドウの期間] に、親マニフェストの総時間 (秒単位) を入力します。
6. [マニフェスト名] に、エンドポイント URL の末尾に付加する文字列を入力します。マニフェスト名により、このエンドポイントにあるマニフェストへの一意のパスを作成できます。HLS マニフェスト名は、新しいエンドポイントの [Manifest name] で指定したマニフェスト名を上書きしません (該当する場合)。
7. (オプション) 他のトラックとともに追加の I フレームのみのストリームをマニフェストに含めるには、[I フレームのみのストリームを含める] を選択します。MediaPackage は、マニフェストの最初のレンディションから I フレーム専用ストリームを生成します。このサービスは EXT-I-FRAMES-ONLY タグを出カマニフェストに挿入し、I フレームのみの再生リストをコンパイルして

それをストリームに含めます。この再生リストでは、早送りや巻き戻しなどのプレイヤー機能を利用できません。

8. (オプション) [プログラムの日付/時間間隔] に、MediaPackage によって EXT-X-PROGRAM-DATE-TIME タグがマニフェストに挿入される間隔 (秒単位) を入力します。

EXT-X-PROGRAM-DATE-TIME タグには、セグメントの時間が保持されます。ソースコンテンツでプログラム日時 (PDT) に関する情報が利用可能な場合、MediaPackage は、それと同じ情報を出力コンテンツにも使用します。それ以外の場合、MediaPackage は PDT に協定世界時 (UTC) を使用します。

PDT 情報は、ダウンストリームプレイヤーがストリームをウォールクロックに同期させるのに役立ちます。それにより、視聴者が再生タイムラインでシークしたり、プレイヤーで時間を表示したりするなどの機能が有効になります。

9. (オプション) [プレイリストタイプ] で、[なし]、[イベント]、[VOD] のいずれかを選択します。イベントまたは VOD として指定すると、対応する EXT-X-PLAYLIST-TYPE エントリがメディア再生リストに含まれます。プレイリストが live to VOD コンテンツであるかどうかを示します。

10. (オプション) 次のフィールドを使用して、MediaPackage が入カストリームからの SCTE-35 メッセージを、どのように処理するかを指示します。詳細については、「[AWS Elemental MediaPackage の SCTE-35 メッセージオプション](#)」を参照してください。

- a. (オプション) [広告マーカ] で、パッケージ化したコンテンツに広告マーカを含める方法を選択します。

次から選択します。

- [None] (なし) – すべての SCTE-35 広告マーカを出カから省きます。
- パススルー – SCTE-35 広告マーカを、入力 HLS の入カストリームから出力に直接コピーします。
- SCTE-35 Enhanced – 入カストリームの SCTE-35 入カメッセージに基づいて、出力で広告マーカとブラックアウトタグを生成します。
- 日付範囲 – 広告やプログラムの移行を知らせるために HLS および CMAF マニフェストで EXT-X-DATERANGE タグを出カします。

- b. (オプション) [広告トリガ] で、出力で広告マーカとして扱う SCTE-35 メッセージタイプを選択します。ここでの選択を行わない場合、MediaPackage は、以下のメッセージタイプに基づいた広告マーカを出カマニフェストに挿入します。

- スプライス挿入
- プロバイダー広告

- デイストリビューター広告
  - プロバイダー配置機会
  - デイストリビューター配置機会
- c. (オプション) [配信制限に関する広告] で、SCTE-35 メッセージのセグメンテーション記述子内の配信制限フラグに基づいて MediaPackage が実行する広告挿入アクションを選択します。
- [None] (なし) – MediaPackage は、出カマニフェストに広告マーカースを挿入しません。
  - [Restricted] (制限あり) – [Customize ad triggers] (広告トリガーをカスタマイズ) で指定した、SCTE-35 メッセージタイプでの配信制限がある場合に、MediaPackage は広告マーカースを挿入します。
  - [Unrestricted] (制限なし) – [Customize ad triggers] (広告トリガーをカスタマイズ) で指定した、SCTE-35 メッセージタイプでの配信制限がない場合に、MediaPackage は広告マーカースを挿入します。
  - [Both] (両方) – [Customize ad triggers] (広告トリガーをカスタマイズ) で指定した、SCTE-35 メッセージタイプでの配信制限があるかどうかにかかわらず、MediaPackage は広告マーカースを挿入します。

## パッケージの暗号化フィールド

コンテンツ暗号化とデジタル著作権管理 (DRM) によって、コンテンツを不正使用から保護します。AWS Elemental MediaPackage は [AWS Secure Packager and Encoder Key Exchange \(SPEKE\) API](#) を使用して、DRM プロバイダーによるコンテンツの暗号化と復号化を容易にします。SPEKE を使用する DRM プロバイダーは、SPEKE API を通じて MediaPackage に暗号化キーを提供します。同時に DRM プロバイダーは、サポートしているメディアプレイヤー用に復号化のためのライセンスも提供します。クラウドで実行されているサービスや機能での SPEKE の使用については、Secure Packager and Encoder Key Exchange API Specification guide の「[AWS cloud-based architecture](#)」を参照してください。

### Important

コンテンツを暗号化するには、DRM プロバイダーと、AWS SPEKE のいずれかのバージョンを使用する必要があります。MediaPackage で暗号化を使用する方法の詳細については、「[AWS Elemental MediaPackage でのコンテンツの暗号化と DRM](#)」を参照してください。

暗号化の値を定義します。

1. 著作権保護なしでコンテンツを提供するには、[No encryption] (暗号化なし) を選択したままにします。
2. 著作権を保護してコンテンツを提供するには、[Encrypt content (コンテンツの暗号化)] を選択して追加のフィールドに以下のように入力します。
  - a. [Resource ID] (リソース ID) で、コンテンツの識別子を入力します。この ID は、現在のエンドポイントを特定するために、サービスよりキーサーバーに送信されます。この設定を、どの程度特異なものにするかは、どの程度詳細なアクセス制御を求めるかによって異なります。このサービスでは、同時に実行される 2 つの暗号化プロセスで、同じ ID を使用することはできません。リソース ID は、コンテンツ ID と呼ばれます。

以下に、リソース ID の例を示します。

```
MovieNight20171126093045
```

- b. [System IDs] (システム ID) に、ストリーミングプロトコルと DRM システムの一意的識別子を入力します。最大 3 つの ID を指定します。複数のシステム ID を指定する場合は、1 行に 1 つずつ入力して、[Add] (追加) をクリックします。ID がわからない場合は、システムプロバイダーにお問い合わせください。
- c. [URL] に、キーサーバーと通信するためにセットアップした API Gateway プロキシの URL を入力します。API Gateway プロキシは、MediaPackage と同じ AWS リージョンに置かれている必要があります。

次は、その URL の例です。

```
https://1wm2dx1f33.execute-api.us-west-2.amazonaws.com/SpekeSample/copyProtection
```

- d. [Role ARN] (ロール ARN) で、API Gateway を介してリクエストを送信するためのアクセス権限を付与する、IAM ロールの Amazon リソースネーム (ARN) を入力します。これは、DRM ソリューションプロバイダーから取得します。

以下は、ロール ARN の例です。

```
arn:aws:iam::444455556666:role/SpekeAccess
```

- e. (オプション) [SPEKE バージョン] で、暗号化に使用する SPEKE のバージョンを選択します。SPEKE バージョン 1.0 は CPIX バージョン 2.0 を使用するレガシーバージョンであり、単一キーによる暗号化をサポートしています。SPEKE バージョン 2.0 では CPIX バージョン 2.3 が使用されており、複数のキーによる暗号化がサポートされます。MediaPackage で SPEKE



を使用する方法の詳細については、「[MediaPackage でのコンテンツの暗号化と DRM](#)」を参照してください。

[SPEKE Version 2.0] (SPEKE バージョン 2.0) を選択した場合には、[Video encryption preset] (ビデオ暗号化プリセット) と [Audio encryption preset] (オーディオ暗号化プリセット) も選択します。このビデオおよびオーディオのプリセット設定により、MediaPackage がストリーム内のビデオとオーディオのトラックを暗号化する際に使用する、コンテンツキーが決定します。これらのプリセットの詳細については、「[SPEKE バージョン 2.0 のプリセット](#)」を参照してください。

SPEKE バージョン 2.0 を使用する場合、MediaPackage ではキーのローテーションが無効化されます。

- f. [Certificate ARN] (証明書 ARN) – (オプション) コンテンツキーでの暗号化に使用する 2048 RSA 証明書 ARN を入力します。このオプションは、DRM キープロバイダーがコンテンツキーの暗号化をサポートしている場合にのみ使用してください。キープロバイダーがサポートしていない場合は、この暗号化を使用してもイベントが失敗します。

ここに証明書 ARN を入力するには、対応する証明書を AWS Certificate Manager に既にインポートしている必要があります。その上で ACM からの証明書 ARN をここに入力します。

コンテンツキーの暗号化については、「[コンテンツキーで使用する証明書の準備と管理](#)」を参照してください。

- g. [暗号化方法] で、CMAF Apple HLS FairPlay の場合は [Sample-AES]を、Microsoft PlayReady と Google Widevine の場合は [AES-CTR]を選択します。
- h. (オプション) [Constant initialization vector] (定数初期化ベクトル) に、コンテンツを暗号化するためのキーで使用される、128 ビット (16 バイト) の 16 進値を、32 文字の文字列により入力します。
- i. (オプション) [Key rotation interval] (キーローテーションの間隔) に、コンテンツがリアルタイムでストリーミングされるライブワークフローでの、キーの変更頻度を秒単位で入力します。サービスは、ライブコンテンツのストリーミングを開始する前にコンテンツキーを取得します。その後は、必要に応じてワークフローの存続期間中にそれらを取得します。デフォルトでは、キーのローテーションは 60 秒間隔に設定されています (60 を設定するのと同じです)。キーのローテーションを無効にするには、この間隔を 0 (ゼロ) に設定します。

次の設定例では、サービスは 30 分ごとにキーのローテーションを実行します。

1800



キーローテーションについては、「[キーローテーションの動作について](#)」を参照してください。

## アクセスコントロールの設定フィールド

アクセスコントロールの値を定義します。

1. このエンドポイントでリクエスト側デバイスにコンテンツを提供できるようにするには、[オリジンを許可する] を選択します。エンドポイントで配信を禁止することは一般的ではありません。

通常、エンドポイントでのコンテンツの提供を禁止するのは、エンドポイントがライブストリームからの VOD コンテンツの収集専用に使われている場合のみです。詳細については、「[AWS Elemental MediaPackage を使用した live-to-VOD アセットの作成](#)」を参照してください。

2. [すべての受信クライアントを許可する] を選択してすべてのリクエスト側 IP アドレスと IP 範囲にコンテンツを提供するか、[IP アドレスによる制限] を選択してこのエンドポイントが提供する IP アドレスを制限します。IP アドレスによって制限する場合は、[IP 許可リスト] に、このエンドポイントでコンテンツを提供する IP アドレスと IP 範囲を入力します。1 行に 1 つの CIDR ブロックです。
3. [CDN 認証の使用] を選択して、このエンドポイントへのコンテンツリクエストに有効な認証コードを含めなければならないようにします。
4. (オプション) [シークレットロール ARN] に、MediaPackage に対して AWS Secrets Manager へのアクセス権限を付与する IAM ロールの ARN を入力します。シークレットロール ARN は次の形式である必要があります: `arn:aws:iam::accountID:role/name`
5. (オプション) [CDN 識別子シークレット ARN] に、CDN がエンドポイントへのアクセス承認に使用する Secrets Manager での認証コードシークレットの ARN を入力します。CDN 識別子は次の形式である必要があります: `arn:aws:secretsmanager:region:accountID:secret:guid`

この認証の仕組みについては、「[AWS Elemental MediaPackage での CDN 認証](#)」を参照してください。

## ストリーム選択に関するフィールド

含めるストリームを定義します。

最小値と最大値で考慮されるのは、ビデオのビットレートのみです。動画ビットレートが指定した最小値未満の場合、他のトラックの総ビットレートに関係なく、その動画は出力に含まれません。同様

に、ビデオのビットレートが、指定した最大値未満の場合、他のトラックの総ビットレートに関係なしに、ビデオは出力に含まれます。

1. (オプション) [ストリームの順序] で、プレイヤーに表示される動画ビットレートの順序を選択します。
  - Original (オリジナル) : 着信ソースと同じ順に従って出カストリームをソートします。
  - 動画ビットレート昇順: 最小のビットレートから開始して最大のビットレートで終わるように出カストリームをソートします。
  - 動画ビットレート降順: 最大のビットレートから開始して最小のビットレートで終わるように出カストリームをソートします。
2. (オプション) [最小動画ビットレート] に、このエンドポイントから再生可能な動画トラックの要件とする最小ビットレート (1 秒あたりのビット数) を入力します。
3. (オプション) [最大動画ビットレート] に、このエンドポイントから再生可能な動画トラックの要件とする最大ビットレート (1 秒あたりのビット数) を入力します。

## チャンネルに関連付けられたすべてのエンドポイントの表示

特定のチャンネルに関連付けられているすべてのエンドポイントを表示し、コンテンツがすべての必要なストリーム形式で利用できることを確認します。

チャンネルに関連付けられているエンドポイントを表示するには、AWS Elemental MediaPackage コンソール、AWS CLI、MediaPackage API を使用できます。AWS CLI または MediaPackage API を使用してエンドポイントを表示する方法については、[AWS Elemental MediaPackage API リファレンス](#)を参照してください。

チャンネルのエンドポイントを表示するには (コンソール)

1. エンドポイントが関連付けられているチャンネルにアクセスします。手順については、「[チャンネルの詳細の表示](#)」を参照してください。

MediaPackage により、すべての既存のエンドポイントがテーブルまたは個別のカードとして表示されます。

2. (オプション) 表示設定 (表示するページのサイズやプロパティなど) を調整するには、[詳細設定] を選択します。

## 単一のエンドポイントの表示

特定のエンドポイントの詳細を表示して、その再生 URL を取得し、現在使用されているパッケージ設定を確認します。

エンドポイントの詳細を表示するには、AWS Elemental MediaPackage コンソール、AWS CLI、MediaPackage API を使用できます。AWS CLI または MediaPackage API を使用してエンドポイントの詳細を確認する方法については、[AWS Elemental MediaPackage API リファレンス](#)を参照してください。

単一のエンドポイントの詳細を表示するには (コンソール)

1. エンドポイントが関連付けられているチャンネルにアクセスします。手順については、「[チャンネルの詳細の表示](#)」を参照してください。
2. チャンネルの詳細ページの [オリジンエンドポイント] で、パッケージ情報や再生プレビューなどの詳細を表示するエンドポイントの ID を選択します。ダウンストリームデバイスのリクエストでは、[Endpoint URL] (エンドポイント URL) フィールドに設定したエンドポイントの URL、または CloudFront の CDN URL を指定する必要があります。

## エンドポイントの編集

エンドポイントのパッケージング設定を編集し、視聴体験を最適化します。エンドポイントの保存後は、パッケージタイプを変更できません。エンドポイントを別のパッケージで保存するには、別のエンドポイントを作成します。

チャンネルを編集して AWS Elemental MediaPackage コンソールからの Amazon CloudFront デイストリビューションの作成を有効化している場合は、エンドポイントを編集してオリジンをデイストリビューションに追加することもできます (まだ別の方法で追加していない場合)。エンドポイントを編集し保存すると、MediaPackage と CloudFront が自動的に連携して、オリジンを作成します。

エンドポイントの設定を変更するには、AWS Elemental MediaPackage コンソール、AWS CLI、MediaPackage API を使用できます。AWS CLI または MediaPackage API を使用してエンドポイントを編集する方法については、[AWS Elemental MediaPackage API リファレンス](#)を参照してください。

エンドポイントの編集に、[名前] フィールドのような自由記述のフィールドに顧客アカウント番号などの機密扱いの識別情報を入力しないようにしてください。これは、コンソール、MediaPackage API、AWS CLI、AWS SDK を使用して MediaPackage を操作する場合も同様です。MediaPackage

に入力するデータはすべて、取得され、診断ログもしくは Amazon CloudWatch Events に含まれる場合があります。

エンドポイントを編集するには (コンソール)

1. エンドポイントが関連付けられているチャンネルにアクセスします。手順については、「[チャンネルの詳細の表示](#)」を参照してください。
2. チャンネルの詳細ページの [オリジンエンドポイント] で、エンドポイント ID を選択し、[エンドポイントを管理] を選択します。
3. 変更するエンドポイントオプションを編集します。

エンドポイントの属性の詳細については、「[エンドポイントの作成](#)」を参照してください。

4. [Save (保存)] を選択します。

## エンドポイントの削除

エンドポイントは、削除されるまでコンテンツを提供できます。エンドポイントが再生リクエストに応答しないようにする場合は、このエンドポイントを削除します。チャンネルのすべてのエンドポイントを削除すると、チャンネル自体を削除できます。

### Warning

エンドポイントを削除すると、再生 URL は機能しなくなります。

エンドポイントを削除するには、AWS Elemental MediaPackage コンソール、AWS CLI、MediaPackage API を使用できます。AWS CLI または MediaPackage API を使用してエンドポイントを削除する方法については、[AWS Elemental MediaPackage API リファレンス](#)を参照してください。

エンドポイントを削除するには (コンソール)

1. エンドポイントが関連付けられているチャンネルにアクセスします。手順については、「[チャンネルの詳細の表示](#)」を参照してください。
2. チャンネルの詳細ページの [オリジンエンドポイント] で、削除するオリジンエンドポイントを選択します。
3. [削除] を選択します。

4. [エンドポイントの削除] の確認ダイアログボックスで、[削除] を選択します。

## エンドポイントのプレビュー

エンドポイントの再生をプレビューし、AWS Elemental MediaPackage でコンテンツストリームが受信されていてパッケージ化できることを確認します。プレビューは、エンドポイントを発行した後の再生エラーの回避と、後で再生の問題が発生した場合のトラブルシューティングに役立ちます。

エンドポイントでの再生をプレビューするには、MediaPackage コンソールを使用します。

エンドポイントの再生をプレビューするには (コンソール)

1. エンドポイントが関連付けられているチャンネルにアクセスします。手順については、「[チャンネルの詳細の表示](#)」を参照してください。
2. チャンネルの詳細ページの [オリジンエンドポイント] で、プレビューするオリジンエンドポイントを選択します。
3. 再生をプレビューするには、次のいずれかの操作を行います。
  - [プレビュー] を選択し、埋め込みプレイヤーでコンテンツを再生します。
  - [QR code] (QR コード) を選択し、互換性があるデバイスで再生の QR コードを表示およびスキャンします。

# AWS Elemental MediaPackage からの VOD コンテンツの配信

AWS Elemental MediaPackage では、ビデオオンデマンド (VOD) コンテンツに以下のリソースを使用します。

- パッケージンググループは、1 つ以上のパッケージング設定を保持しています。グループでは、1 つのアセットに同時に複数の出力設定を適用できます。1 つのグループに複数のアセットを関連付け、すべてのアセットで出力の設定が同じになるようにできます。
- パッケージング設定では、MediaPackage でアセットからの出力をパッケージ化する方法を指定できます。この設定では、暗号化、ビットレート、およびパッケージング設定を定義します。
- アセットでは、ソースコンテンツを取り込み、再生リクエストに対してパッケージング設定が動的に適用されます。

サポートされている VOD 入力とコーデックについては、「[VOD でサポートされるコーデックおよび入力タイプ](#)」を参照してください。

次のセクションでは、これらのリソースを使用して MediaPackage で VOD コンテンツを管理する方法について説明します。

## トピック

- [AWS Elemental MediaPackage でパッケージグループを使用する](#)
- [AWS Elemental MediaPackage でパッケージ設定を使用する](#)
- [AWS Elemental MediaPackage でアセットを使用する](#)

## AWS Elemental MediaPackage でパッケージグループを使用する

パッケージグループには、1 つ以上のパッケージング設定が保持されています。パッケージグループがアセットに関連付けられている場合、パッケージグループ設定によってアセットから使用可能な出力が定義されます。複数のアセットを 1 つのパッケージグループに関連付けることができます。これにより、同じ設定を複数のアセットに適用できます。

## トピック

- [パッケージグループの作成](#)

- [パッケージグループの詳細の表示](#)
- [パッケージンググループの編集](#)
- [パッケージンググループの削除](#)
- [パッケージンググループへのパッケージング設定の追加](#)

## パッケージグループの作成

アセットのすべてのパッケージ設定を保持するためのパッケージグループを作成します。パッケージグループでは、例えば Apple HLS および DASH-ISO をサポートするデバイスへの出力にアセットが利用可能であることを AWS Elemental MediaPackage に伝えることができます。

パッケージグループを作成するときに、CDN 認証を有効にするオプションがあります。CDN 認証の詳細については、「[AWS Elemental MediaPackage での CDN 認証](#)」を参照してください。

パッケージグループの作成には、MediaPackage コンソール、AWS CLI、MediaPackage API を使用できます。AWS CLI または MediaPackage API を使用したパッケージグループの作成については、AWS Elemental MediaPackage VOD API リファレンスの「[Packaging\\_groups](#)」を参照してください。

パッケージグループの作成中に、[ID] フィールドのような自由記述のフィールドに顧客アカウント番号などの機密扱いの識別情報を入力しないようにしてください。これは、MediaPackage コンソール、MediaPackage API、AWS CLI、AWS SDK を使用している場合に該当します。MediaPackage に入力したデータはすべて取得され、診断ログまたは Amazon CloudWatch Events に包含される場合があります。

パッケージグループを作成するには (コンソール)

1. MediaPackage コンソール (<https://console.aws.amazon.com/mediapackage/>) を開きます。
2. ナビゲーションペインの、[Video on demand] で、[Packaging group (パッケージンググループ)] を選択します。
3. [パッケージグループ] ページで [グループを作成] を選択します。
4. [Creating packaging group] ダイアログボックスで、以下の操作を行います。
  1. [ID] に、パッケージグループを説明する名前を入力します。ID は、グループのプライマリ識別子であり、この AWS リージョン 内のアカウントに対して一意である必要があります。
  2. [作成] を選択します。



MediaPackage で新しいパッケージグループの詳細ページが表示されます。

パッケージグループの作成中にアカウントのクォータを超えると、エラーが発生します。「リクエストが多すぎます。もう一度試してください」といったエラーが表示されます。リソース制限の超過のエラーが出力される場合は、API リクエストのクォータを超過したか、使用しているパッケージンググループの数が、アカウントで許される上限に既に到達しています。これが最初のグループであるか、このエラーが誤って表示されたと思われる場合は、Service Quotas コンソールを使用して、[クォータの引き上げをリクエスト](#)してください。MediaPackage でのクォータの詳細については、「[AWS Elemental MediaPackage のクォータ](#)」を参照してください。

## パッケージグループの詳細の表示

AWS Elemental MediaPackage に設定されているすべてのパッケージグループのほか、関連付けられているパッケージ設定など特定のパッケージグループの詳細を表示できます。

パッケージグループの詳細を表示するには、AWS Elemental MediaPackage コンソール、AWS CLI、MediaPackage API を使用できます。AWS CLI または MediaPackage API を使用してパッケージグループを表示する方法については、AWS Elemental MediaPackage VOD API リファレンスの「[Packaging\\_groups id](#)」を参照してください。

パッケージグループを表示するには (コンソール)

1. MediaPackage コンソール (<https://console.aws.amazon.com/mediapackage/>) を開きます。
2. ナビゲーションペインの、[Video on demand] で、[Packaging group (パッケージンググループ)] を選択します。

すべてのグループがコンソールに表示されます。

3. 特定のパッケージンググループに関する詳細情報を表示するには、グループの名前を選択してください。

MediaPackage により、このパッケージグループに関連付けられているアセットなどの概要情報が表示されます。

## パッケージンググループの編集

パッケージンググループを編集して、アクセスコントロール設定を設定します。

**Note**

パッケージンググループの作成後、パッケージンググループ ID を編集することはできません。パッケージンググループ ID を変更する場合は、新しいパッケージンググループを作成する必要があります。

AWS Elemental MediaPackage コンソール、AWS CLI、MediaPackage API を使用して、パッケージンググループのアクセスコントロール設定を編集できます。AWS CLI または MediaPackage API を使用してパッケージンググループを編集する方法については、[MediaPackage VOD API リファレンス](#) を参照してください。

## パッケージンググループの削除

AWS Elemental MediaPackage がアセットからそれ以上のコンテンツを配信しないようにするには、パッケージンググループを削除します。パッケージンググループを削除する前に、そのグループのパッケージ設定およびそのグループを使用しているアセットをすべて削除する必要があります。

- パッケージング設定を削除するには「[パッケージング設定の削除](#)」を参照してください。
- アセットを削除するには、「[アセットの削除](#)」を参照してください。

パッケージ設定の削除には、MediaPackage コンソール、AWS CLI、MediaPackage API を使用できます。AWS CLI または MediaPackage API を使用してパッケージンググループを削除する方法については、AWS Elemental MediaPackage VOD API リファレンスの「[Packaging\\_groups id](#)」を参照してください。

パッケージンググループを削除するには (コンソール)

1. MediaPackage コンソール (<https://console.aws.amazon.com/mediapackage/>) を開きます。
2. ナビゲーションペインの、[Video on demand] で、[Packaging group (パッケージンググループ)] を選択します。
3. [パッケージンググループ] ページで、削除するパッケージンググループを選択します。
4. [Delete] (削除) をクリックします。
5. [パッケージンググループの削除] ダイアログボックスで、[削除] を選択してパッケージンググループの削除を終了します。

## パッケージンググループへのパッケージング設定の追加

AWS Elemental MediaPackage がアセットからの出力をどのようにフォーマットするかを定義するには、パッケージング設定をパッケージンググループに追加します。

パッケージンググループにパッケージ設定を追加するには、MediaPackage コンソール、AWS CLI、MediaPackage API を使用できます。AWS CLI または MediaPackage API を使用してパッケージ設定を追加する方法については、AWS Elemental MediaPackage VOD API リファレンスの「[Packaging\\_configurations](#)」を参照してください。

MediaPackage コンソールからパッケージンググループにパッケージング設定を追加する手順については、「[パッケージング設定の作成](#)」を参照してください。

## AWS Elemental MediaPackage でパッケージ設定を使用する

パッケージング設定は、アセットの単一の配信ポイントを定義します。この設定には、プレイヤーまたは Amazon などのコンテンツ配信ネットワーク (CDN) と AWS Elemental MediaPackage 統合するために必要なすべての情報が保持されます CloudFront。設定では、以下のいずれかのストリーム形式で出力コンテンツに設定します。

- Apple HLS – コンテンツを Apple HTTP Live Streaming (HLS) 用にパッケージ化
- Microsoft Smooth – コンテンツを Microsoft Smooth Streaming プレーヤー用にパッケージ化
- Common Media Application Format (CMAF) – コンテンツを Apple HLS fragmented MP4 (fMP4) をサポートするデバイス用にパッケージ化
- DASH-ISO – コンテンツを DASH-ISO ABR ストリーミングプロトコル用にパッケージ化

パッケージング設定にはデジタル著作権管理 (DRM)、暗号化統合、ビットレートの表示順などに関する情報も保持されます。

### トピック

- [パッケージング設定の作成](#)
- [パッケージ設定に関する詳細の表示](#)
- [パッケージング設定の編集](#)
- [パッケージング設定の削除](#)

## パッケージング設定の作成

AWS Elemental MediaPackage がアセットからの配信用にコンテンツを準備する方法を定義するためのパッケージ設定を作成します。

パッケージング設定を作成するには、MediaPackage コンソール、AWS CLI または MediaPackage API を使用します。AWS CLI または MediaPackage API を使用してパッケージング設定を作成する方法については、AWS Elemental MediaPackage VOD API リファレンスの「[Packaging configurations](#)」を参照してください。

パッケージング設定の作成中に、[ID] フィールドのような自由記述のフィールドにお客様のアカウント番号などの機密扱いの識別情報を置かないようにしてください。これは、MediaPackage コンソール、MediaPackage API、AWS CLI または AWS SDKs を使用している場合に適用されます。に入力したデータはすべて、診断ログまたは Amazon CloudWatch Events に取り込まれる MediaPackage 可能性があります。

### トピック

- [HLS 向けパッケージング設定の作成](#)
- [DASH 向けパッケージ設定の作成](#)
- [Microsoft Smooth 向けパッケージング設定の作成](#)
- [CMAF パッケージ設定の作成](#)

## HLS 向けパッケージング設定の作成

Apple HLS をサポートするデバイス向けにコンテンツをフォーマットするパッケージング設定を作成します。

Apple HLS パッケージング設定を作成するには (コンソール)

1. <https://console.aws.amazon.com/mediapackage/> で MediaPackage コンソールを開きます。
2. ナビゲーションペインの、[Video on demand] で、[Packaging group (パッケージンググループ)] を選択します。
3. [Packaging groups (パッケージンググループ)] ページで、作成している設定を含めるグループを選択します。
4. パッケージグループの詳細ページの [パッケージ設定] で、[設定を管理] を選択します。
5. [パッケージ設定を管理] ページの [パッケージ設定] で、[追加] をクリックし、[新しい設定] を選択します。

6. 以下のトピックの説明に従ってフィールドに入力します。

- [全般的な設定に関するフィールド](#)
- [マニフェスト設定に関するフィールド](#)
- [ストリーム選択に関するフィールド](#)
- [暗号化に関するフィールド](#)

7. [保存] を選択します。

パッケージ設定を作成しているときにアカウントのクォータを超えると、エラーが発生します。

「リクエストが多すぎます。もう一度試してください。」、といったエラーが表示されます。リソース制限の超過のエラーが出力される場合は、API リクエストのクォータを超過したか、使用しているパッケージンググループの数が、アカウントで許される上限に既に到達しています。これが最初のグループであるか、このエラーが誤って表示されたと思われる場合は、Service Quotas コンソールを使用して、[クォータの引き上げをリクエスト](#)してください。のクォータの詳細については MediaPackage、[「](#)」を参照してください [AWS Elemental MediaPackage のクォータ](#)。

### 全般的な設定に関するフィールド

設定パッケージ全体に適用される全般設定を指定します。

1. [ID] に、設定を説明する名前を入力します。ID は、設定のプライマリ識別子であり、AWS リージョン内のアカウントに対して一意である必要があります。
2. [Package type (パッケージタイプ)] で、[Apple HLS] を選択します。
3. (オプション) [Segment duration (セグメント時間)] に、各セグメントの時間 (秒単位) を入力します。入力セグメントの長さと同じか、その倍数の値を入力します。入力した値が入力セグメント時間と異なる場合、AWS Elemental MediaPackage は最も近いセグメント時間の倍数にセグメントを切り捨てます。

### マニフェスト設定に関するフィールド

AWS Elemental MediaPackage がこのパッケージ設定を使用するアセットから配信するマニフェストの形式を指定します。

1. (オプション) [Manifest name (マニフェスト名)] に、エンドポイント URL に付加する短い文字列を入力します。マニフェスト名は、このエンドポイントへの一意のパスをします。値を入力しないと、MediaPackage はデフォルトのマニフェスト名 index を使用します。

2. (オプション) IFrame のみのストリームを含めるを選択して、追加の I フレームのみのストリームと manifest の他のトラックを含めます。は、マニフェストの最初のレンディションから I フレームのみのストリーム MediaPackage を生成します。サービスは EXT-I-FRAMES-ONLY タグを出カマニフェストに挿入し、I フレーム専用再生リストを生成した上で、それをストリームを含めます。この再生リストでは、早送りや巻き戻しなどのプレイヤー機能を利用できます。
3. (オプション) すべてのオーディオトラックを 1 つの HLS レンディショングループにまとめるには、[オーディオレンディショングループを使用] を選択します。レンディショングループの詳細については、「[AWS Elemental MediaPackage のレンディショングループのリファレンス](#)」を参照してください。
4. (オプション) 毎回マニフェストのセグメントの前に、サービスに同じキーを繰り返させたい場合は、[Repeat EXT-X-KEY] (EXT-X-KEY を繰り返す) を選択します。デフォルトでは、キーは、ヘッダーの後、セグメントの前に一度だけ書き込まれます。[Repeat EXT-X-KEY] (EXT-X-KEY を繰り返す) を選択すると、マニフェストはすべてのセグメントにキーが前置される形式で (ヘッダー、キー、セグメント、キー、セグメント、キー... のように) 記述されます。この設定は、プレイヤーの要件に合わせて行ってください。このオプションを選択すると、DRM サーバーへのクライアントリクエストが増える場合があります。
5. (オプション) デジタルビデオ放送 (DVB) の字幕を出カにパススルーするには、[DVB 字幕を含める] を選択します。
6. (オプション) プログラムの日付/時間間隔には、がマニフェストに EXT-X-PROGRAM-DATE-TIME タグを挿入 MediaPackage する間隔 (秒単位) を入力します。  
  
EXT-X-PROGRAM-DATE-TIME タグは、ストリームとウォールクロックを同期させ、再生タイムラインでの視聴者によるシークやプレーヤーでの時刻表示などの機能を有効にします。
7. (オプション) [広告マーカ―] で、パッケージ化したコンテンツに広告マーカ―を含める方法を選択します。

次から選択します。

- [None] (なし) – すべての SCTE-35 広告マーカ―を出カから省きます。
- パススルー – SCTE-35 広告マーカ―を、入力 HLS の入カストリームから出カに直接コピーします。
- SCTE-35 Enhanced – 入カストリームの SCTE-35 入カメッセージに基づいて広告マーカ―とブラックアウトタグを生成します。

## ストリーム選択に関するフィールド

再生可能な受信ビットレートを制限し、このパッケージ設定を使用するアセットの出力でストリームを並べ替えます。

最小値と最大値で考慮されるのは、ビデオのビットレートのみです。動画ビットレートが指定した最小値未満の場合、他のトラックの総ビットレートに関係なく、その動画は出力に含まれません。同様に、ビデオのビットレートが、指定した最大値未満の場合、他のトラックの総ビットレートに関係なしに、ビデオは出力に含まれます。

最小ビットレートと最大ビットレートを設定して出力をソートするには、[ストリームの選択を有効にする] を選択して次のように追加フィールドに入力します。

1. (オプション) [Stream order] (ストリーム順) で、以下から選択します。
  - Original (オリジナル): 着信ソースと同じ順に従って出カストリームをソートします。
  - [昇順]: 最低のビットレートから開始して最高のビットレートで終わるように出カストリームをソートします。
  - [降順]: 最高のビットレートから開始して最低のビットレートで終わるように出カストリームをソートします。
2. (オプション) [最小動画ビットレート] に、このエンドポイントから再生可能な動画トラックの要件とする最小ビットレートのしきい値 (1 秒あたりのビット数) を入力します。これにより、トラックが一定のビットレート以上になります。
3. (オプション) [最大動画ビットレート] に、このエンドポイントから再生可能な動画トラックの要件とする最大ビットレートのしきい値 (1 秒あたりのビット数) を入力します。これにより、トラックが一定のビットレートを超えないようになります。

## 暗号化に関するフィールド

コンテンツ暗号化とデジタル著作権管理 (DRM) によって、コンテンツを不正使用から保護します。AWS Elemental MediaPackage は [AWS Secure Packager and Encoder Key Exchange \(SPEKE\) API](#) を使用して、DRM プロバイダーによるコンテンツの暗号化と復号化を容易にします。SPEKE を使用すると、DRM プロバイダーは SPEKE API MediaPackage を通じて暗号化キーを に提供します。同時に DRM プロバイダーは、サポートしているメディアプレーヤー用に復号化のためのライセンスも提供します。クラウドで実行されているサービスや機能での SPEKE の使用については、Secure Packager and Encoder Key Exchange API Specification guide の「[AWS cloud-based architecture](#)」を参照してください。



**Note**

コンテンツを暗号化するには、DRM ソリューションプロバイダーが必要で、暗号化を使用するように設定する必要があります。詳細については、[the section called “コンテンツの暗号化と DRM”](#) を参照してください。

著作権を保護してコンテンツを提供するには、[暗号化を有効化] を選択して追加のフィールドに以下のように入力します。

1. 暗号化方法 で、Apple HLS の場合は Sample-AES、Apple HLS FairPlay の場合は AES-128 を選択します。AES-128
2. (オプション) [Constant initialization vector] (定数初期化ベクトル) に、コンテンツを暗号化するためのキーで使用される、128 ビット (16 バイト) の 16 進値を、32 文字の文字列により入力します。
3. [URL] に、キーサーバーと通信するためにセットアップした API Gateway プロキシの URL を入力します。API Gateway プロキシは、AWS リージョンと同じに存在する必要があります MediaPackage。

次は、その URL の例です。

```
https://1wm2dx1f33.execute-api.us-west-2.amazonaws.com/SpekeSample/copyProtection
```

4. [Role ARN] (ロール ARN) で、API Gateway を介してリクエストを送信するためのアクセス権限を付与する、IAM ロールの Amazon リソースネーム (ARN) を入力します。これは、DRM ソリューションプロバイダーから取得します。

以下は、ロール ARN の例です。

```
arn:aws:iam::444455556666:role/SpekeAccess
```

5. [System IDs] (システム ID) に、ストリーミングプロトコルと DRM システムの一意的識別子を入力します。CMAF には最大 3 つの ID、DASH には 2 つの ID、その他、残りのストリーミングプロトコルには 1 つの ID をそれぞれ指定します。複数のシステム ID を指定する場合は、1 行に 1 つずつ入力して、[Add] (追加) クリックします。一般的なシステム ID のリストについては、「[DASH-IF システム ID](#)」を参照してください。ID がわからない場合は、DRM ソリューションプロバイダーにお尋ねください。

## DASH 向けパッケージ設定の作成

DASH-ISO をサポートするデバイス用にコンテンツをフォーマットするパッケージ設定を作成します。

DASH-ISO パッケージ設定を作成するには (コンソール)

1. <https://console.aws.amazon.com/mediapackage/> で MediaPackage コンソールを開きます。
2. ナビゲーションペインの、[Video on demand] で、[Packaging group (パッケージンググループ)] を選択します。
3. [Packaging groups (パッケージンググループ)] ページで、作成している設定を含めるグループを選択します。
4. パッケージグループの詳細ページの [パッケージ設定] で、[設定を管理] を選択します。
5. [パッケージ設定を管理] ページの [パッケージ設定] で、[追加] と [新しい設定] を選択します。
6. 以下のトピックの説明に従ってフィールドに入力します。

- [全般的な設定に関するフィールド](#)
- [マニフェスト設定に関するフィールド](#)
- [ストリーム選択に関するフィールド](#)
- [暗号化に関するフィールド](#)

7. [保存] を選択します。

パッケージ設定を作成しているときにアカウントのクォータを超えると、エラーが発生します。「リクエストが多すぎます。もう一度試してください。」、といったエラーが表示されます。リソース制限の超過のエラーが出力される場合は、API リクエストのクォータを超過したか、使用しているパッケージンググループの数が、アカウントで許される上限に既に到達しています。これが最初のグループであるか、このエラーが誤って表示されたと思われる場合は、Service Quotas コンソールを使用して、[クォータの引き上げをリクエスト](#)してください。のクォータの詳細については MediaPackage、[「」を参照してください](#)[AWS Elemental MediaPackage のクォータ](#)。

### 全般的な設定に関するフィールド

設定パッケージ全体に適用される全般設定を指定します。

1. [ID] に、設定を説明する名前を入力します。ID は、設定のプライマリ識別子であり、リージョン内のアカウント別に一意であることが必要です。

2. [Package type (パッケージタイプ)] で、[DASH-ISO] を選択します。
3. (オプション) [Segment duration (セグメント時間)] に、各セグメントの時間 (秒単位) を入力します。入力セグメントの長さと同じか、その倍数の値を入力します。入力した値が入力セグメント時間と異なる場合、AWS Elemental MediaPackage は最も近いセグメント時間の倍数にセグメントを切り捨てます。

## マニフェスト設定に関するフィールド

AWS Elemental MediaPackage がこのパッケージ設定を使用するアセットから配信するマニフェストの形式を指定します。


1. (オプション) [Manifest name (マニフェスト名)] に、エンドポイント URL に付加する短い文字列を入力します。マニフェスト名により、このエンドポイントへの一意のパスを作成できます。値を入力しない場合、デフォルトのマニフェスト名は index です。
2. (オプション) [Min buffer time (最小バッファ時間)] に、プレーヤーがバッファに保持する必要がある最小時間 (秒単位) を入力します。ネットワーク条件のせいで再生が中断する場合は、再生が失敗する前に追加のコンテンツがプレーヤーにバッファされ、視聴者に影響が及ばないように復旧時間が確保されます。
3. (オプション) [プロファイル] で、DASH プロファイルを指定します。

次から選択します。

- [None] (なし) – 出力で DASH プロファイルを使用しない
  - Hbbtv 1.5 – 出力は HbbTV v1.5 に準拠します。HbbTV v1.5 の詳細については、[HbbTV の仕様に関するウェブサイト](#)を参照してください。
4. (オプション) マニフェストレイアウト で、再生リクエストに応じてフル、圧縮、または DRM の最上位圧縮マニフェスト MediaPackage を提供するかどうかを選択します。
    - [Full (完全)] を選択した場合、MediaPackage はマニフェストのすべての Representation について、SegmentTemplate および SegmentTimeline タグを提供します。
    - [Compact (圧縮)] を選択した場合、MediaPackage は重複した SegmentTemplate タグをまとめ、マニフェストの先頭で提供します。これによりマニフェストが短くなり、一部のデバイスで処理が容易になります。
    - DRM の最上位圧縮 を選択した場合、 はコンテンツ保護要素をメディアプレゼンテーションの説明 (MPD) レベル MediaPackage に配置し、AdaptationSet レベルで参照します。このオプションは、SPEKE バージョン 1.0 または 2.0 SHARED プリセットを使用している場合にのみ選択できます。

マニフェストのレイアウトオプションの詳細については、「[圧縮された DASH マニフェスト](#)」を参照してください。

- (オプション) セグメントテンプレート形式で、MediaPackage および 再生リクエストが各セグメントを参照する方法を選択します。
  - [Number with timeline (タイムライン付きの番号)] を選択した場合、MediaPackage は \$Number\$ 変数を使用して、SegmentTemplate タグの media 属性のセグメントを参照します。変数の値はセグメントの連続番号です。SegmentTimeline は各セグメントテンプレートに含まれています。
  - [Time with timeline (タイムライン付き時間)] を選択した場合、MediaPackage はセグメントを参照するために \$Time\$ 変数を使用します。変数の値は、マニフェストタイムライン上でセグメントが開始されるときのタイムスタンプです。SegmentTimeline は各セグメントテンプレートに含まれています。
  - [Number with duration (期間付き番号)] を選択すると、MediaPackage は、\$Number\$ 変数を使用して SegmentTimeline オブジェクトをセグメントテンプレートの duration 属性と置き換えます。

 Note

このオプションは、複数期間 DASH と組み合わせて使用することはできません。

SegmentTemplate タグの書式設定オプションの詳細については、「[DASH マニフェストのセグメントテンプレート形式](#)」を参照してください。

- (オプション) IFrame のみのストリームを含めるを選択して、追加の I フレームのみのストリームと manifest の他のトラックを含めます。は、マニフェストの最初のレンディションから I フレームのみのストリーム MediaPackage を生成します。この再生リストでは、早送りや巻き戻しなどのプレイヤー機能を利用できます。
- 期間トリガーでは、が DASH 出カマニフェストで MPD 期間 MediaPackage を作成する方法を選択します。
  - None – MediaPackage 追加の期間を作成しません。マニフェストを 1 つの期間としてフォーマットし、このセグメントには SCTE-35 マーカーを含みません。
  - 広告で新しい期間をトリガーする — MediaPackage は、入力コンテンツからの SCTE-35 広告マーカーに基づいて、複数の期間マニフェストを作成して挿入します。これらの期間は、メインコンテンツと広告コンテンツの間の境界コンテンツのように、コンテンツを分割します。マ

ニフェストで **が期間 MediaPackage** を設定する方法の詳細については、「」を参照してください [AWS Elemental MediaPackage の DASH マニフェストオプション](#)。

**⚠ Important**

複数期間は、DASH コンテンツで広告挿入をパーソナライズするために AWS Elemental MediaTailor を使用する場合に必要です。このサービスの詳細については、[AWS Elemental MediaTailor ユーザーガイド](#)を参照してください。

8. [SCTE マーカーのソース] で、入力 HLS コンテンツから使用する SCTE-35 マーカーのソースを指定します。
  - 入力 HLS メディアセグメントから SCTE-35 マーカーを使用するには、[セグメント] を選択します。
  - 入力 HLS 子マニフェストから SCTE-35 Enhanced 構文 (#EXT-OATCLS-SCTE35 タグ) を使用してフォーマットされた SCTE-35 マーカーを使用するには、[マニフェスト] を選択します。SCTE-35 Elemental 構文および SCTE-35 Daterange 構文は、サポートされていません。
9. (オプション) のセグメントにエンコーダ設定を含めるを選択し MediaPackage、init フラグメントではなくすべてのビデオセグメントにエンコーダのシーケンスパラメータセット (TAK)、ピクチャパラメータセット (PPS)、およびビデオパラメータセット (VPS) メタデータを配置します。これにより、コンテンツの再生中、アセットごとに異なる SPS/PPS/VPS 設定を使用できます。

## ストリーム選択に関するフィールド

再生可能な受信ビットレートを制限し、このパッケージ設定を使用するアセットの出力でストリームを並べ替えます。

最小値と最大値で考慮されるのは、ビデオのビットレートのみです。動画ビットレートが指定した最小値未満の場合、他のトラックの総ビットレートに関係なく、その動画は出力に含まれません。同様に、ビデオのビットレートが、指定した最大値未満の場合、他のトラックの総ビットレートに関係なしに、ビデオは出力に含まれます。

最小ビットレートと最大ビットレートを設定して出力をソートするには、[ストリームの選択を有効にする] を選択して次のように追加フィールドに入力します。

1. (オプション) [Stream order] (ストリーム順) で、以下から選択します。
  - Original (オリジナル) : 着信ソースと同じ順に従って出力ストリームをソートします。

- [昇順]: 最低のビットレートから開始して最高のビットレートで終わるように出力ストリームをソートします。
  - [降順]: 最高のビットレートから開始して最低のビットレートで終わるように出力ストリームをソートします。
2. (オプション) [最小動画ビットレート] に、このエンドポイントから再生可能な動画トラックの要件とする最小ビットレートのしきい値 (1 秒あたりのビット数) を入力します。これにより、トラックが一定のビットレート以上になります。
  3. (オプション) [最大動画ビットレート] に、このエンドポイントから再生可能な動画トラックの要件とする最大ビットレートのしきい値 (1 秒あたりのビット数) を入力します。これにより、トラックが一定のビットレートを超えないようになります。

## 暗号化に関するフィールド

コンテンツ暗号化とデジタル著作権管理 (DRM) によって、コンテンツを不正使用から保護します。AWS Elemental MediaPackage は [AWS Secure Packager and Encoder Key Exchange \(SPEKE\) API](#) を使用して、DRM プロバイダーによるコンテンツの暗号化と復号化を容易にします。SPEKE を使用すると、DRM プロバイダーは SPEKE API MediaPackage を通じて暗号化キーを に提供します。同時に DRM プロバイダーは、サポートしているメディアプレイヤー用に復号化のためのライセンスも提供します。クラウドで実行されているサービスや機能での SPEKE の使用については、Secure Packager and Encoder Key Exchange API Specification guide の「[AWS cloud-based architecture](#)」を参照してください。

### Note

コンテンツを暗号化するには、DRM ソリューションプロバイダーが必要で、暗号化を使用するように設定する必要があります。詳細については、[the section called “コンテンツの暗号化と DRM”](#) を参照してください。

著作権を保護してコンテンツを提供するには、[暗号化を有効化] を選択して追加のフィールドに以下のように入力します。

1. [URL] に、キーサーバーと通信するためにセットアップした API ゲートウェイプロキシの URL を入力します。API Gateway プロキシは、AWS リージョンと同じ に存在する必要があります MediaPackage。

次は、その URL の例です。



```
https://1wm2dx1f33.execute-api.us-west-2.amazonaws.com/SpekeSample/copyProtection
```

2. [Role ARN] (ロール ARN) で、API Gateway を介してリクエストを送信するためのアクセス権限を付与する、IAM ロールの Amazon リソースネーム (ARN) を入力します。これは、DRM ソリューションプロバイダーから取得します。

以下は、ロール ARN の例です。

```
arn:aws:iam::444455556666:role/SpekeAccess
```

3. [System IDs] (システム ID) に、ストリーミングプロトコルと DRM システムの一意的識別子を入力します。CMAF には最大 3 つの ID、DASH には 2 つの ID、その他、残りのストリーミングプロトコルには 1 つの ID をそれぞれ指定します。複数のシステム ID を指定する場合は、1 行に 1 つずつ入力して、[Add] (追加) クリックします。一般的なシステム ID のリストについては、「[DASH-IF システム ID](#)」を参照してください。ID がわからない場合は、DRM ソリューションプロバイダーにお尋ねください。
4. (オプション) [SPEKE バージョン] で暗号化に使用する SPEKE のバージョンを選択します。SPEKE バージョン 1.0 は CPIX バージョン 2.0 を使用するレガシーバージョンであり、単一キーによる暗号化をサポートしています。SPEKE バージョン 2.0 では CPIX バージョン 2.3 が使用されており、複数のキーによる暗号化がサポートされます。で SPEKE を使用方法の詳細については MediaPackage、「[でのコンテンツの暗号化と DRM MediaPackage](#)」を参照してください。

[SPEKE Version 2.0] (SPEKE バージョン 2.0) を選択した場合には、[Video encryption preset] (ビデオ暗号化プリセット) と [Audio encryption preset] (オーディオ暗号化プリセット) も選択します。ビデオプリセットとオーディオプリセットは、ガストリーム内のオーディオトラックとビデオトラックの暗号化 MediaPackage に使用するコンテンツキーを決定します。これらのプリセットの詳細については、「[SPEKE バージョン 2.0 のプリセット](#)」を参照してください。

SPEKE バージョン 2.0 を使用する場合、はキーローテーションを MediaPackage 無効にします。

## Microsoft Smooth 向けパッケージング設定の作成

Microsoft Smooth をサポートするデバイス用にコンテンツをフォーマットするパッケージ設定を作成します。



## Microsoft Smooth パッケージング設定を作成するには (コンソール)

1. <https://console.aws.amazon.com/mediapackage/> で MediaPackage コンソールを開きます。
2. ナビゲーションペインの、[Video on demand] で、[Packaging group (パッケージンググループ)] を選択します。
3. [Packaging groups (パッケージンググループ)] ページで、作成している設定を含めるグループを選択します。
4. パッケージグループの詳細ページの [パッケージ設定] で、[設定を管理] を選択します。
5. [パッケージ設定を管理] ページの [パッケージ設定] で、[追加] をクリックし、[新しい設定] を選択します。
6. 以下のトピックの説明に従ってフィールドに入力します。
  - [全般的な設定に関するフィールド](#)
  - [マニフェスト設定に関するフィールド](#)
  - [ストリーム選択に関するフィールド](#)
  - [暗号化に関するフィールド](#)
7. [保存] を選択します。

パッケージ設定を作成しているときにアカウントのクォータを超えると、エラーが発生します。「リクエストが多すぎます。もう一度試してください。」、といったエラーが表示されます。「リソース制限の超過」というエラーが表示される場合は、API リクエストのクォータを超過しているか、使用しているパッケージグループの数がアカウントで許される上限に既に到達しています。これが最初のグループであるか、このエラーが誤って表示されたと思われる場合は、Service Quotas コンソールを使用して、[クォータの引き上げをリクエスト](#)してください。MediaPackage のクォータの詳細については、「[AWS Elemental MediaPackage のクォータ](#)」を参照してください。

### 全般的な設定に関するフィールド

設定パッケージ全体に適用される全般設定を指定します。

1. [ID] に、設定を説明する名前を入力します。ID は、設定のプライマリ識別子であり、リージョン内のアカウント別に一意であることが必要です。
2. [Package type (パッケージタイプ)] で、[Microsoft Smooth] を選択します。
3. (オプション) [Segment duration (セグメント時間)] に、各セグメントの時間 (秒単位) を入力します。入力セグメントの長さと同じか、その倍数の値を入力します。入力した値が入力セグメント

時間と異なる場合、AWS Elemental MediaPackage は最も近いセグメント時間の倍数にセグメントを切り捨てます。

## マニフェスト設定に関するフィールド

AWS Elemental MediaPackage がこのパッケージ設定を使用するアセットから配信するマニフェストの形式を指定します。

- (オプション) [Manifest name (マニフェスト名)] に、エンドポイント URL に付加する短い文字列を入力します。マニフェスト名により、このエンドポイントへの一意のパスを作成できます。値を入力しない場合、デフォルトのマニフェスト名は index です。

## ストリーム選択に関するフィールド

再生可能な受信ビットレートを制限し、このパッケージ設定を使用するアセットの出力でストリームを並べ替えます。

最小値と最大値で考慮されるのは、ビデオのビットレートのみです。動画ビットレートが指定した最小値未満の場合、他のトラックの総ビットレートに関係なく、その動画は出力に含まれません。同様に、ビデオのビットレートが、指定した最大値未満の場合、他のトラックの総ビットレートに関係なしに、ビデオは出力に含まれます。

最小ビットレートと最大ビットレートを設定して出力をソートするには、[ストリームの選択を有効にする] を選択して次のように追加フィールドに入力します。

1. (オプション) [Stream order] (ストリーム順) で、以下から選択します。
  - Original (オリジナル): 着信ソースと同じ順に従って出力ストリームをソートします。
  - [昇順]: 最低のビットレートから開始して最高のビットレートで終わるように出力ストリームをソートします。
  - [降順]: 最高のビットレートから開始して最低のビットレートで終わるように出力ストリームをソートします。
2. (オプション) [最小動画ビットレート] に、このエンドポイントから再生可能な動画トラックの要件とする最小ビットレートのしきい値 (1 秒あたりのビット数) を入力します。これにより、トラックが一定のビットレート以上になります。
3. (オプション) [最大動画ビットレート] に、このエンドポイントから再生可能な動画トラックの要件とする最大ビットレートのしきい値 (1 秒あたりのビット数) を入力します。これにより、トラックが一定のビットレートを超えないようになります。

## 暗号化に関するフィールド

コンテンツ暗号化とデジタル著作権管理 (DRM) によって、コンテンツを不正使用から保護します。AWS Elemental MediaPackage は [AWS Secure Packager and Encoder Key Exchange \(SPEKE\) API](#) を使用して、DRM プロバイダーによるコンテンツの暗号化と復号化を容易にします。SPEKE を使用すると、DRM プロバイダーは SPEKE API MediaPackage を通じて暗号化キーを に提供します。同時に DRM プロバイダーは、サポートしているメディアプレイヤー用に復号化のためのライセンスも提供します。クラウドで実行されているサービスや機能での SPEKE の使用については、Secure Packager and Encoder Key Exchange API Specification guide の「[AWS cloud-based architecture](#)」を参照してください。

### Note

コンテンツを暗号化するには、DRM ソリューションプロバイダーが必要で、暗号化を使用するように設定する必要があります。詳細については、[the section called “コンテンツの暗号化と DRM”](#) を参照してください。

著作権を保護してコンテンツを提供するには、[暗号化を有効化] を選択して追加のフィールドに以下のように入力します。

1. [URL] に、キーサーバーと通信するためにセットアップした API ゲートウェイプロキシの URL を入力します。API Gateway プロキシは、AWS リージョンと同じに存在する必要があります MediaPackage。

次は、その URL の例です。

```
https://1wm2dx1f33.execute-api.us-west-2.amazonaws.com/SpekeSample/copyProtection
```

2. [Role ARN] (ロール ARN) で、API Gateway を介してリクエストを送信するためのアクセス権限を付与する、IAM ロールの Amazon リソースネーム (ARN) を入力します。これは、DRM ソリューションプロバイダーから取得します。

以下は、ロール ARN の例です。

```
arn:aws:iam::444455556666:role/SpekeAccess
```

3. [System IDs] (システム ID) に、ストリーミングプロトコルと DRM システムの一意的識別子を入力します。CMAF には最大 3 つの ID、DASH には 2 つの ID、その他、残りのストリーミング

プロトコルには 1 つの ID をそれぞれ指定します。複数のシステム ID を指定する場合は、1 行に 1 つずつ入力して、[Add] (追加) クリックします。一般的なシステム ID のリストについては、「[DASH-IF システム ID](#)」を参照してください。ID がわからない場合は、DRM ソリューションプロバイダーにお尋ねください。

## CMAF パッケージ設定の作成

Apple HLS fragmented MP4 (fMP4) をサポートするデバイス向けにコンテンツをフォーマットするパッケージング設定を作成します。

CMAF パッケージ設定を作成するには (コンソール)

1. <https://console.aws.amazon.com/mediapackage/> で MediaPackage コンソールを開きます。
2. ナビゲーションペインの、[Video on demand] で、[Packaging group (パッケージンググループ)] を選択します。
3. [Packaging groups (パッケージンググループ)] ページで、作成している設定を含めるグループを選択します。
4. パッケージグループの詳細ページの [パッケージ設定] で、[設定を管理] を選択します。
5. [パッケージ設定を管理] ページの [パッケージ設定] で、[追加] をクリックし、[新しい設定] を選択します。
6. 以下のトピックの説明に従ってフィールドに入力します。
  - [全般的な設定に関するフィールド](#)
  - [マニフェスト設定に関するフィールド](#)
  - [ストリーム選択に関するフィールド](#)
  - [暗号化に関するフィールド](#)
7. [保存] を選択します。

パッケージ設定を作成しているときにアカウントのクォータを超えると、エラーが発生します。「リクエストが多すぎます。もう一度試してください。」、といったエラーが表示されます。リソース制限の超過のエラーが出力される場合は、API リクエストのクォータを超過したか、使用しているパッケージンググループの数が、アカウントで許される上限に既に到達しています。これが最初のグループであるか、このエラーが誤って表示されたと思われる場合は、Service Quotas コンソールを使用して、[クォータの引き上げをリクエスト](#)してください。のクォータの詳細については MediaPackage、「[」を参照してください](#)[AWS Elemental MediaPackage のクォータ](#)。

## 全般的な設定に関するフィールド

設定パッケージ全体に適用される全般設定を指定します。

1. [ID] に、設定を説明する名前を入力します。ID は、設定のプライマリ識別子であり、リージョン内のアカウント別に一意であることが必要です。
2. [Package type (パッケージタイプ)] で、[Common Media Application Format (CMAF)] を選択します。
3. (オプション) [Segment duration (セグメント時間)] に、各セグメントの時間 (秒単位) を入力します。入力セグメントの長さと同じか、その倍数の値を入力します。入力した値が入力セグメント時間と異なる場合、AWS Elemental MediaPackage は最も近いセグメント時間の倍数にセグメントを切り捨てます。

## マニフェスト設定に関するフィールド

AWS Elemental MediaPackage がこのパッケージ設定を使用するアセットから配信するマニフェストの形式を指定します。

1. (オプション) [Manifest name (マニフェスト名)] に、エンドポイント URL に付加する短い文字列を入力します。マニフェスト名は、このエンドポイントへの一意のパスをします。値を入力しないと、MediaPackage はデフォルトのマニフェスト名 `index` を使用します。
2. (オプション) 1 つの動画トラックを使用したストリームセットで、他のトラックと合わせて追加の I フレームのみのストリームをマニフェストに含める場合は、[I Frame のみのストリームを含める] を選択します。MediaPackage はマニフェストに `EXT-I-FRAMES-ONLY` タグを挿入し、I フレームのみのプレイリストをコンパイルしてストリームに含めます。この再生リストでは、早送りや巻き戻しなどのプレイヤー機能を利用できます。
3. (オプション) 毎回マニフェストのセグメントの前に、サービスに同じキーを繰り返させたい場合は、[Repeat EXT-X-KEY] (EXT-X-KEY を繰り返す) を選択します。デフォルトでは、キーは、ヘッダーの後、セグメントの前に一度だけ書き込まれます。[Repeat EXT-X-KEY] (EXT-X-KEY を繰り返す) を選択すると、マニフェストはすべてのセグメントにキーが前置される形式で (ヘッダー、キー、セグメント、キー、セグメント、キー... のように) 記述されます。この設定は、プレイヤーの要件に合わせて行ってください。このオプションを選択すると、DRM サーバーへのクライアントリクエストが増える場合があります。
4. (オプション) プログラムの日付/時間間隔 に、 がマニフェストに `EXT-X-PROGRAM-DATE-TIME` タグを挿入 MediaPackage する間隔を入力します。

EXT-X-PROGRAM-DATE-TIME タグは、ストリームとウォールクロックを同期させ、再生タイムラインでの視聴者によるシークやプレーヤーでの時刻表示などの機能を有効にします。

5. (オプション) [広告マーカ―] で、パッケージ化したコンテンツに広告マーカ―を含める方法を選択します。

次から選択します。

- [None] (なし) – すべての SCTE-35 広告マーカ―を出力から省きます。
  - パススルー – SCTE-35 広告マーカ―を、入力 HLS の入カストリームから出力に直接コピーします。
  - SCTE-35 Enhanced – 入カストリームの SCTE-35 入カメッセージに基づいて広告マーカ―とラックアウトタグを生成します。
6. (オプション) セグメントにエンコーダ設定を含める を選択し、MediaPackage が init フラグメントではなくすべてのビデオセグメントにエンコーダのシーケンスパラメータセット (TAK)、ピクチャパラメータセット (PPS)、およびビデオパラメータセット (VPS) メタデータを配置します。これにより、コンテンツの再生中、アセットごとに異なる SPS/PPS/VPS 設定を使用できます。

## ストリーム選択に関するフィールド

再生可能な受信ビットレートを制限し、このパッケージ設定を使用するアセットの出力でストリームを並べ替えます。

最小値と最大値で考慮されるのは、ビデオのビットレートのみです。動画ビットレートが指定した最小値未満の場合、他のトラックの総ビットレートに関係なく、その動画は出力に含まれません。同様に、ビデオのビットレートが、指定した最大値未満の場合、他のトラックの総ビットレートに関係なしに、ビデオは出力に含まれます。

最小ビットレートと最大ビットレートを設定して出力をソートするには、[ストリームの選択を有効にする] を選択して次のように追加フィールドに入力します。

1. (オプション) [Stream order] (ストリーム順) で、以下から選択します。
  - Original (オリジナル): 着信ソースと同じ順に従って出力ストリームをソートします。
  - [昇順]: 最低のビットレートから開始して最高のビットレートで終わるように出力ストリームをソートします。
  - [降順]: 最高のビットレートから開始して最低のビットレートで終わるように出力ストリームをソートします。



2. (オプション) [最小動画ビットレート] に、このエンドポイントから再生可能な動画トラックの要件とする最小ビットレートのしきい値 (1 秒あたりのビット数) を入力します。これにより、トラックが一定のビットレート以上になります。
3. (オプション) [最大動画ビットレート] に、このエンドポイントから再生可能な動画トラックの要件とする最大ビットレートのしきい値 (1 秒あたりのビット数) を入力します。これにより、トラックが一定のビットレートを超えないようになります。

## 暗号化に関するフィールド

コンテンツ暗号化とデジタル著作権管理 (DRM) によって、コンテンツを不正使用から保護します。AWS Elemental MediaPackage は [AWS Secure Packager and Encoder Key Exchange \(SPEKE\) API](#) を使用して、DRM プロバイダーによるコンテンツの暗号化と復号化を容易にします。SPEKE を使用すると、DRM プロバイダーは SPEKE API MediaPackage を通じて暗号化キーを に提供します。同時に DRM プロバイダーは、サポートしているメディアプレイヤー用に復号化のためのライセンスも提供します。クラウドで実行されているサービスや機能での SPEKE の使用については、Secure Packager and Encoder Key Exchange API Specification guide の「[AWS cloud-based architecture](#)」を参照してください。

### Note

コンテンツを暗号化するには、DRM ソリューションプロバイダーが必要で、暗号化を使用するように設定する必要があります。詳細については、[the section called “コンテンツの暗号化と DRM”](#) を参照してください。

著作権を保護してコンテンツを提供するには、[暗号化を有効化] を選択して追加のフィールドに以下のように入力します。

1. [System IDs] (システム ID) に、ストリーミングプロトコルと DRM システムの一意的識別子を入力します。最大 2 つのシステム ID を指定します。複数のシステム ID を指定する場合は、1 行に 1 つずつ入力します。ID がわからない場合は、DRM ソリューションプロバイダーにお問い合わせください。
2. [URL] に、キーサーバーと通信するためにセットアップした API Gateway プロキシの URL を入力します。API Gateway プロキシは、AWS リージョンと同じに存在する必要があります MediaPackage。

次は、その URL の例です。



```
https://1wm2dx1f33.execute-api.us-west-2.amazonaws.com/SpekeSample/copyProtection
```

3. (オプション) [SPEKE バージョン] で暗号化に使用する SPEKE のバージョンを選択します。SPEKE バージョン 1.0 は CPIX バージョン 2.0 を使用するレガシーバージョンであり、単一キーによる暗号化をサポートしています。SPEKE バージョン 2.0 では CPIX バージョン 2.3 が使用されており、複数のキーによる暗号化がサポートされます。SPEKE を使用方法の詳細については MediaPackage、[「でのコンテンツの暗号化と DRM MediaPackage」](#) を参照してください。

[SPEKE Version 2.0] (SPEKE バージョン 2.0) を選択した場合には、[Video encryption preset] (ビデオ暗号化プリセット) と [Audio encryption preset] (オーディオ暗号化プリセット) も選択します。ビデオプリセットとオーディオプリセットは、ガストリーム内のオーディオトラックとビデオトラックの暗号化 MediaPackage に使用するコンテンツキーを決定します。これらのプリセットの詳細については、[「SPEKE バージョン 2.0 のプリセット」](#) を参照してください。

SPEKE バージョン 2.0 を使用する場合は、キーローテーションを MediaPackage 無効にします。

4. (オプション) [Constant initialization vector (定数初期化ベクトル)] に、コンテンツを暗号化するためのキーで使用される、128 ビット (16 バイト) の 16 進値を 32 文字の文字列により入力します。
5. [Role ARN] (ロール ARN) で、API Gateway を介してリクエストを送信するためのアクセス権限を付与する、IAM ロールの Amazon リソースネーム (ARN) を入力します。これは、DRM ソリューションプロバイダーから取得します。

以下は、ロール ARN の例です。

```
arn:aws:iam::444455556666:role/SpekeAccess
```

## パッケージ設定に関する詳細の表示

特定のパッケージンググループまたはアセットに関連付けられているすべてのパッケージング設定を表示し、コンテンツがすべての必要なストリーム形式で利用可能であることを確認します。

パッケージング設定を表示するには、AWS Elemental MediaPackage コンソール、AWS CLI または MediaPackage API を使用します。AWS CLI または MediaPackage API を使用してパッケージング設定を表示する方法については、AWS Elemental MediaPackage VOD API リファレンスの [「Packaging\\_configurations id」](#) を参照してください。

## パッケージグループのパッケージング設定を表示するには (コンソール)

1. <https://console.aws.amazon.com/mediapackage/> で MediaPackage コンソールを開きます。
2. ナビゲーションペインの、[Video on demand] で、[Packaging group (パッケージンググループ)] を選択します。
3. [Packaging groups (パッケージンググループ)] ページで、表示する設定を含めるグループを選択します。

[Packaging configurations (パッケージ設定)] セクションに、このグループに含まれるすべての設定が表示されます。

4. 特定のパッケージ設定の詳細を表示するには、その設定の [Id] を選択します。

MediaPackage は、このパッケージング設定に関連付けられたアセットなどの概要情報を表示します。

## アセットに関連付けられているすべてのパッケージング設定を表示するには (コンソール)

1. <https://console.aws.amazon.com/mediapackage/> で MediaPackage コンソールを開きます。
2. ナビゲーションペインの、[Video on demand] で、[Assets (アセット)] を選択します。
3. [Assets (アセット)] ページで、監査するアセットを選択します。

[Playback details (再生の詳細)] セクションには、このアセットに関連付けられているすべての設定が表示されます。このページの [Status] (ステータス) 列で、アセットの再生ステータスを確認することができます。表示可能なステータスは以下のとおりです。

- [Not processed] (未処理) – アセットはまだ処理されていません。
- Processing - MediaPackage アセットを処理しています。アセットは、まだ再生可能な状態ではありません。
- [Processed] (処理済み) – アセットの処理が完了し再生可能な状態です。
- [Failed] (失敗) – 処理に失敗しました。

### Note

2021年9月30日より前に取り込まれたほとんどのアセットでは、ステータス情報は利用できません。

## パッケージング設定の編集

パッケージング設定を編集することはできません。変更が必要な場合は、新しい設定を作成して元の設定を削除してください。

- 設定を作成するには、「[パッケージング設定の作成](#)」を参照してください。
- 設定を削除するには、「[パッケージング設定の削除](#)」を参照してください。

## パッケージング設定の削除

アセットから再生エンドポイントを削除するには、パッケージ設定を削除します。

パッケージング設定を削除するには、AWS Elemental MediaPackageコンソール、AWS CLIまたはMediaPackage APIを使用します。AWS CLIまたはMediaPackage APIを使用してパッケージング設定を削除する方法については、AWS Elemental MediaPackageVOD API リファレンスの「[Packaging\\_configurations id](#)」を参照してください。

パッケージング設定を削除するには (コンソール)

1. <https://console.aws.amazon.com/mediapackage/> で MediaPackage コンソールを開きます。
2. ナビゲーションペインの、[Video on demand] で、[Packaging group (パッケージンググループ)] を選択します。
3. [Packaging groups (パッケージンググループ)] ページで、削除する設定を含めるグループを選択します。
4. パッケージグループの詳細ページの [パッケージ設定] で、削除する設定のパッケージ設定 ID を選択して [削除] を選択するか、[設定を管理]、[アクション]、[削除] を選択します。
5. [パッケージ設定の削除] ページで、[削除] を選択します。

## AWS Elemental MediaPackage でアセットを使用する

アセットは、MediaPackage が Amazon S3 などのソースからファイルベースの動画コンテンツを取り込むために必要なすべての情報を保持します。アセットを通じて、MediaPackage は再生リクエストに応じてコンテンツを取り込み、動的にパッケージ化します。アセットに関連付けられた設定によって、アセットを出力用にパッケージ化する方法が決まります。

アセットを取り込むと、AWS Elemental MediaPackage はアセットに関連付けられている各再生設定の URL を提供します。この URL は、長期にわたって発生する可能性のある失敗に関係なく、ア

セットの有効期間中は固定されています。ダウンストリームデバイスはこの URL を使用して再生リクエストを送信します。

サポートされている VOD 入力とコーデックについては、「[VOD でサポートされるコーデックおよび入力タイプ](#)」を参照してください。

トピック

- [アセットの取り込み](#)
- [アセットの詳細の表示](#)
- [アセットの編集](#)
- [アセットの削除](#)

## アセットの取り込み

ソースコンテンツを取り込むには、AWS Elemental MediaPackage でアセットを作成します。コンテンツを取り込んだ MediaPackage は、アセットに関連付けられているすべてのパッケージング設定ごとに、一意の再生 URL を生成します。

### Important

アセットを取得する MediaPackage には、ソースコンテンツが保存されている Amazon S3 バケットへのアクセスが許可されている必要があります。適切なアクセス許可を MediaPackage に付与するロールを作成するには、「[他の AWS サービスへのアクセスを AWS Elemental MediaPackage に許可する](#)」を参照してください。

アセットは、MediaPackage コンソール、AWS CLI、MediaPackage API を使用して作成できます。AWS CLI または MediaPackage API を使用したパッケージ設定の作成方法については、AWS Elemental MediaPackage VOD API リファレンスの「[Assets](#)」を参照してください。

アセットの作成中に、[ID] フィールドのような自由記述のフィールドにお客様のアカウント番号などの機密扱いの識別情報を置かないようにしてください。これは、MediaPackage コンソール、MediaPackage API、AWS CLI、AWS SDK を使用している場合に該当します。MediaPackage に入力するデータはすべて、取得され、診断ログもしくは Amazon CloudWatch Events に包含される場合があります。

## アセットを取り込むには (コンソール)

1. MediaPackage コンソール (<https://console.aws.amazon.com/mediapackage/>) を開きます。
2. ナビゲーションペインの、[Video on demand] で、[Assets (アセット)] を選択します。
3. [アセット] ページで、[アセットを取り込む] を選択します。
4. [アセットを取り込む] ページで、以下のトピックの説明に従ってフィールドに入力します。
  - [アセットのアクセスに関するフィールド](#)
  - [アセットの詳細に関するフィールド](#)
  - [パッケージング設定に関するフィールド](#)
5. [アセットの取り込み] を選択します。

VOD アセットの取り込みは非同期アクションです。アセットが再生可能な状態になるまでに要する時間は、アセットの持続時間やアセットの複雑さなど、いくつかの要因によって異なります。CloudWatch の VodAssetPlayable イベントをモニタリングすることで、VOD アセットで再生の準備ができたタイミングを追跡できます。このイベントは、アセットが再生できる状態になった時点で、MediaPackage から送信されます。詳細については、「[VOD Playback Events](#)」を参照してください。


パッケージ設定を作成しているときにアカウントのクォータを超えると、エラーが発生します。「リクエストが多すぎます。もう一度試してください。」、といったエラーが表示されます。リソース制限の超過のエラーが出力される場合は、API リクエストのクォータを超過したか、使用しているパッケージンググループの数が、アカウントで許される上限に既に到達しています。これが最初のグループであるか、このエラーが誤って表示されたと思われる場合は、Service Quotas コンソールを使用して、[クォータの引き上げをリクエスト](#)してください。MediaPackage でのクォータの詳細については、「[AWS Elemental MediaPackage のクォータ](#)」を参照してください。

## アセットのアクセスに関するフィールド

以下の各フィールドは、AWS Elemental MediaPackage が Amazon S3 バケット内のソースコンテンツに、どのようにアクセスするのかを指定します。MediaPackage にはバケットにアクセスするためのアクセス許可が必要です。適切なアクセス許可を持つ IAM ロールを作成するには、「[他の AWS サービスへのアクセスを AWS Elemental MediaPackage に許可する](#)」を参照してください。

1. [Amazon S3 バケット名] で、MediaPackage がアカウントで検出したバケットのリストから選択するか、バケットの名前を入力します。Amazon S3 バケットは、MediaPackage が取り込んで再生用にパッケージ化するソースコンテンツを保持します。バケットの名前を入力した場


合、MediaPackage にはこのバケットに対する可視性がないため、バケットに互換性があるかどうかはわかりません。

 Note

Amazon S3 バケットを表示するアクセスが許可されていない場合は、MediaPackage にこのオプションは表示されません。AWS 管理者に連絡するか、または [Specify bucket name (バケット名を指定する)] フィールドに手動でバケット名を入力してください。

2. [IAM ロール] で、Amazon S3 バケットから読み取るための MediaPackage アクセス権のある IAM ロールを選択します。

- MediaPackage がアカウントから検出したロールをリストの中から選択するには、[Use existing role] (既存のロールを使用する) をクリックし、ロールを選択します。

 Note

IAM ロールを表示するアクセス権がない場合、MediaPackage にこのオプションは表示されません。AWS 管理者に連絡するか、[Specify custom role name (カスタムロール名を指定する)] フィールドに手動でロール ARN を入力します。

- MediaPackage が検出していないロールを使用するには、[Specify custom role name] をクリックし、ロールのカスタム ARN を入力します。MediaPackage には、このロールに対する可視性がないため、このロールにより適切なアクセス許可の提供が可能かどうかは判別していません。

## アセットの詳細に関するフィールド

以下のフィールドは、このアセットが使用するソースコンテンツを説明しています。

このアセットに複数のソースがある場合は、[Add asset (アセットの追加)] を選択してフィールドに入力します。すべてのソースコンテンツに対してこれを行います。

 Important

ソースコンテンツは、smil (MP4) または m3u8 (HLS/TS) ファイル形式にする必要があります。



1. [ファイル名] に、Amazon S3 バケット内の.smil マニフェスト (MP4) または.m3u8 親プレイリスト (HLS) への完全なパスを、ソースコンテンツの名前を含めて入力します。[S3 bucket name (S3 バケット名)] フィールドで選択したため、バケット名を入力する必要はありません。例えば、lion\_movie.m3u8 という名前のコンテンツが、movies という名前のバケット内の thursday\_night というサブディレクトリに置かれている場合は、次のように [Filename] (ファイル名) フィールドに入力します。

```
thursday_night/lion_movie.m3u8
```

MediaPackage で.smil マニフェストを使用する方法の詳細については、「[.smil マニフェストでの要件](#)」を参照してください。

2. [ID] に、アセットを説明する名前を入力します。ID はアセットの主要な識別子であり、このリージョンのアカウントに対して一意である必要があります。使用できるのは、文字、数字、下線 ( \_ )、ダッシュ ( - ) のみです。
3. (オプション)[リソース ID] に、コンテンツの識別子を入力します。SPEKE を使用している場合、リソース ID はキーサーバーがコンテンツを参照するために使用する識別子となります。MediaPackage は、現在のアセットを識別するために ID をキーサーバーに送信します。ID を一意にする方法は、必要なアクセスコントロールのレベルによって異なります。このサービスでは、2 つの同時の暗号化プロセスに同じ ID を使用することはできません。リソース ID は、コンテンツ ID と呼ばれます。

#### Example

```
MovieNight20171126093045
```

## パッケージング設定に関するフィールド

以下のフィールドは、AWS Elemental MediaPackage がこのアセットからの出力をどのようにパッケージ化するかを決定します。

- [グループのパッケージ化] で、このアセットに使用する設定を保持しているグループを選択します。グループのパッケージ化は、再生リクエストに対応するためにコンテンツをパッケージ化する際に MediaPackage で使用されるパッケージ設定を決定します。



## アセットの詳細の表示

AWS Elemental MediaPackage に設定されているすべてのアセット、またはそれに関連付けられているパッケージング設定を含む特定のアセットの詳細を表示できます。

アセットの詳細は、MediaPackage コンソール、AWS CLI、MediaPackage API を使用して表示できます。AWS CLI または MediaPackage API を使用したパッケージ設定の作成方法については、AWS Elemental MediaPackage VOD API リファレンスの「[Assets id](#)」を参照してください。

アセットを表示するには (コンソール)

1. MediaPackage コンソール (<https://console.aws.amazon.com/mediapackage/>) を開きます。
2. ナビゲーションペインの、[Video on demand] で、[Assets (アセット)] を選択します。

すべてのアセットがコンソールに表示されます。

3. 特定のアセットに関する詳細情報を表示するには、アセットの名前を選択してください。

このパッケージングアセットに関連付けられているパッケージ設定や、それらの再生 URL などの概要情報が、MediaPackage により表示されます。

## アセットの編集

アセットを編集することはできません。変更するには、アセットをもう一度取り込み、元のファイルを削除します。

- アセットを取り込むには、「[パッケージング設定の作成](#)」を参照してください。
- アセットを削除するには、「[パッケージング設定の削除](#)」を参照してください。

## アセットの削除

パッケージンググループの URL を削除し、AWS Elemental MediaPackage がそれ以上コンテンツを配信しないようにするには、アセットを削除します。

アセットを削除するには、MediaPackage コンソール、AWS CLI、MediaPackage API を使用できます。AWS CLI または MediaPackage API を使用したパッケージ設定の作成方法については、AWS Elemental MediaPackage VOD API リファレンスの「[Assets id](#)」を参照してください。

## アセットを削除するには (コンソール)

1. MediaPackage コンソール (<https://console.aws.amazon.com/mediapackage/>) を開きます。
2. ナビゲーションペインの、[Video on demand] で、[Assets (アセット)] を選択します。
3. [アセット] ページで、削除するアセットを選択します。
4. [Delete] (削除) をクリックします。

# AWS Elemental MediaPackage を使用した live-to-VOD アセットの作成

Live-to-VOD (ビデオオンデマンド) アセットは、後で再生するために抽出され保存されたライブストリームの一部です。たとえば、ゲームのクリップを保存してゲームのハイライト集に使用したり、ブロードキャスト番組のクリップを保存して後で番組の宣伝に使用したりできます。

MediaPackage で Live-to-VOD アセットを作成するには、収集ジョブリソースを作成します。収集ジョブはリクエストとして作成され、MediaPackage でライブストリームの一部を抽出し、そのクリップを Live-to-VOD アセットとして Amazon S3 バケットに保存するために使用されます。収集ジョブは 1 回のみ実行され、その記録は、MediaPackage によってアカウントに 90 日間保持されます。このレコードは参照専用です。削除または変更することはできません。

## Important

Live-to-VOD アセットを作成するには、Amazon S3 バケットへのアクセスと保存を MediaPackage に許可する必要があります。手順については、「[他の AWS サービスへのアクセスを AWS Elemental MediaPackage に許可する](#)」を参照してください。

以下のトピックでは、MediaPackage の Live-to-VOD アセットについて詳しく説明します。

## トピック

- [Live-to-VOD の要件](#)
- [Live-to-VOD の仕組み](#)
- [収集ジョブの使用](#)

## Live-to-VOD の要件

AWS Elemental MediaPackage で Live-to-VOD アセットを作成する場合は、以下の要件に留意してください。

### エンドポイントの要件

Live-to-VOD アセットを収集するエンドポイントは、以下の要件を満たしている必要があります。

- スタートオーバーを有効にし、同時に [startover window] (スタートオーバーウィンドウ) には 14日以内を設定する必要があります。ウィンドウのサイズを確認または変更するには、「[the section called “単一のエンドポイントの表示”](#)」を参照してください。
- エンドポイントは、クリアな (非暗号化の) または暗号化された、DASH または HLS コンテンツのどちらかを提供する必要があります。
- DASH エンドポイントの場合 – DASH エンドポイントはセグメントテンプレート形式として、[Number with timeline] (タイムライン付き番号)、または[Time with timeline] (タイムライン付き時刻) のいずれかを使用する必要があります。DASH エンドポイントの作成については、「[DASH エンドポイントの作成](#)」を参照してください。
- MediaPackage VOD では現在、暗号化されたアセットの取り込みはサポートされていません。収集したアセットを MediaPackage のビデオオンデマンドのワークフローで使用していて、エンドポイントが暗号化されている場合は、同じチャンネルに暗号化されていないシャドウエンドポイントを作成します。これを行うには、[Allow origination] (配信を許可) を選択解除し、新しいエンドポイントを再生に使用できないようにします。MediaPackage は、配信が有効になっていないエンドポイントの URL を作成しますが、このエンドポイントに送信された再生リクエストに対してはエラーを返します。

## Live-to-VOD アセットの要件

Live-to-VOD アセットは、以下の要件を満たしている必要があります。

- 開始時間は、エンコーダの開始時間以降にする必要があります。
- 開始および終了時間は、エンドポイントのスタートオーバーウィンドウ内であることが必要です。
- その期間は、Live-to-VOD マニフェストの最大長 (24 時間) を超えて設定することはできません。

## Live-to-VOD の仕組み

live-to-VOD (ビデオオンデマンド) コンテンツの処理フローでは、AWS Elemental MediaPackage によってライブコンテンツストリームから動画のクリップが抽出されます。MediaPackage は、このクリップを Live-to-VOD アセットとして Amazon S3 に保存します。アセットを再生デバイスに配信するには、MediaPackage の VOD コンテンツ処理機能を使用します。または、HLS もしくは DASH 入力をサポートする VOD エンコードサービスを使用することもできます。

そのための主要な手順の概要は以下のとおりです。

1. ライブストリームを取り込むチャンネルとエンドポイントを作成し、HLS もしくは DASH 出力用にパッケージ化します。エンドポイントは、「[Live-to-VOD の要件](#)」で概説されている要件を満たしている必要があります。
2. ライブストリームから抽出する Live-to-VOD アセットを定義する収集ジョブを作成します。このアセットも、「Live-to-VOD の要件」で概説されている要件を満たしている必要があります。
3. MediaPackage によって、収集ジョブで指定した期間のアセットが収集されます。アセットはセグメントに忠実です。たとえば、6 秒のセグメントがあり、収集ジョブの開始時間がセグメントの 3 秒である場合、アセットは 3 秒早く、つまりセグメントの開始時に開始されます。

MediaPackage はアセットを収集した後、収集ジョブで指定した Amazon S3 バケットに、そのアセットを保存します。MediaPackage はそのバケット内にディレクトリを作成し、収集ジョブの [Manifest key] (マニフェストキー) で指定した情報に基づいて、親マニフェストに名前を付けます。例えば、マニフェストキーが `thursdaynight/highlights/index.m3u8` の場合、MediaPackage は Amazon S3 バケットに `thursdaynight/highlights` ディレクトリを作成し、親マニフェストに `index.m3u8` という名前を付けます。

MediaPackage は、収集ジョブが完了 (または失敗) した時点で、CloudWatch イベントを作成します。収集ジョブのイベントについては、「[収集ジョブの通知イベント](#)」を参照してください。

MediaPackage はアカウントに、このジョブの読み取り専用の参照を 90 日間保持します。90 日後、MediaPackage はアカウントからジョブのレコードを削除します。この時点で、ワークフローで必要であれば、収集ジョブの ID を再利用できます。

4. この段階で、MediaPackage の Live-to-VOD 機能は完了します。Live-to-VOD アセットは Amazon S3 バケットにあるので、そのアセットを使用してワークフローの目的を達成できます。例えば、MediaPackage の VOD 機能またはエンコーディングサービスを使用して、アセットを再生可能にすることができます。

## 収集ジョブの使用

収集ジョブとは、過去の特定の期間に対応する Live-to-VOD (ビデオオンデマンド) アセットをエンドポイントから抽出するリクエストです。AWS Elemental MediaPackage は、収集ジョブからの情報を使用して、アセットの開始時間と終了時間、および収集ジョブ完了後のアセットの保存場所を決定します。

収集ジョブは作成後に 1 回のみ実行されます。MediaPackage はアカウントに、このジョブの参照専用レコードを保持します。収集ジョブの作成後、そのレコードを変更または削除することはできません。

## トピック

- [収集ジョブの作成](#)
- [収集ジョブの詳細の表示](#)
- [収集ジョブの編集](#)
- [収集ジョブの削除](#)

## 収集ジョブの作成

収集ジョブを作成して、暗号化されている、あるいはクリアな (非暗号化の) HLS もしくは DASH のライブストリームから、Live-to-VOD アセットを抽出します。

### Important

収集ジョブを実行し Live-to-VOD アセットを保存する MediaPackage には、アセットが保存される Amazon S3 バケットにアクセスし書き込むためのアクセス許可が必要です。適切なアクセス許可を MediaPackage に付与するロールを作成するには、「[他の AWS サービスへのアクセスを AWS Elemental MediaPackage に許可する](#)」を参照してください。

収集ジョブは、MediaPackage コンソール、AWS CLI、または MediaPackage API を使用して作成します。AWS CLI または MediaPackage API を使用してジョブを作成する方法については、[AWS Elemental MediaPackage API リファレンス](#) を参照してください。

収集ジョブの作成中に、[ID] フィールドのような自由記述のフィールドにお客様のアカウント番号などの機密扱いの識別情報を入力しないでください。これは、MediaPackage コンソール、MediaPackage API、AWS CLI、AWS SDK を使用している場合に該当します。MediaPackage に入力するデータはすべて、取得され、診断ログもしくは Amazon CloudWatch Events に包含される場合があります。

収集ジョブを作成するには (コンソール)

1. MediaPackage コンソール (<https://console.aws.amazon.com/mediapackage/>) を開きます。
2. ナビゲーションペインの [Live (ライブ)] で、[Harvest jobs (収集ジョブ)] を選択します。
3. [ハーベストジョブ] ページで、[ハーベストジョブの作成] を選択します。
4. [収集ジョブの作成] ページで、以下のトピックで説明しているようにフィールドに入力します。

- [基本的な詳細](#)

- [開始日時と終了日時](#)
- [送信先](#)

5. [Create] (作成) を選択します。

## 基本的な詳細

収集ジョブの基本的な詳細では、そのジョブの ID、および Live-to-VOD アセットのソースを定義します。

1. [ID] に、収集ジョブを説明する名前を入力します。ID は収集ジョブの主要な識別子です。収集ジョブが期限切れになりアカウントから削除された後、そのジョブの ID は再利用できます。使用できるのは、文字、数字、下線 (\_)、ダッシュ (-) のみです。
2. [Origin endpoint (配信エンドポイント)] で、Live-to-VOD アセットを収集するライブストリームを提供するエンドポイントを選択します。

以下の考慮事項に注意してください。

- 収集ジョブは、MediaPackage エンドポイントの [startover window] (スタートオーバーウィンドウ) 内に収まる必要があります。スタートオーバーウィンドウによって、エンドポイントからアセットを収穫できる時間枠が決定されます。例えば、エンドポイントのスタートオーバーウィンドウが 3 日である場合、その期間内であればいつでもアセットを収集できます。

MediaPackage エンドポイントには、ゼロから 14 日の間でスタートオーバーウィンドウを設定できます。エンドポイントのスタートオーバーウィンドウを調整するには、「[単一のエンドポイントの表示](#)」を参照してください。

- 収集した Live-to-VOD アセットの時間長は、最大で 24 時間です。Live-to-VOD アセットの時間長を設定するには、この章の「[開始日時と終了日時](#)」を参照してください。
- エンドポイントは、クリアな (非暗号化の) または暗号化された、DASH または HLS コンテンツのどちらかを提供する必要があります。
- MediaPackage VOD では現在、暗号化されたアセットの取り込みはサポートされていません。収集したアセットを MediaPackage のビデオオンデマンドのワークフローで使用していて、エンドポイントが暗号化されている場合は、同じチャンネルに暗号化されていないシャドウエンドポイントを作成します。これを行うには、[Allow origination] (配信を許可) を選択解除し、新しいエンドポイントを再生に使用できないようにします。MediaPackage は、配信が有効になっていないエンドポイントの URL を作成しますが、このエンドポイントに送信された再生リクエストに対してはエラーを返します。詳細については、「[AWS Elemental MediaPackage を使用した live-to-VOD アセットの作成](#)」を参照してください。



## 開始日時と終了日時

開始日時と終了日時の情報は、収集ジョブの時間範囲を定義します。収集ジョブ実行の最大期間は24時間です。時間は、エンコーダーからのプログラム日時 (PDT) に基づきます。

### Note

Live-to-VOD アセットのタイミングはセグメントに忠実です。つまり、セグメントの範囲に収まる開始時間と終了時間を指定すると、MediaPackage はセグメント全体をアセットに含めます。3 秒のセグメントがあり、開始時間がセグメントの 3 秒である場合、アセットは 3 秒早く、つまりセグメントの開始時に開始されます。

- [Date and time format (日付と時刻の形式)] で、Live-to-VOD アセットの開始時間と終了時間を示すために使用する形式を選択します。
  - 現地時間 - 日付と時刻は現在のブラウザセッションの設定に従った形式になります。現地時間には 24 時間制が使用されます。
  - エポック秒 - 日付と時刻はエポックからの秒数の形式になります。
  - ISO-8601 - 日付と時刻は ISO-8601 標準に従った形式になります。
- [When the live-to-VOD asset begins] に、live-to-VOD アセットの開始日時を入力します。アセットの開始時間はライブイベントの開始以降であることが必要です。開始時間はエンドポイントのスタートオーバーウィンドウ内であることも必要です。エンドポイントのウィンドウが 5 時間であり、開始時間が 6 時間前である場合、収集ジョブは失敗します。
- [When the live-to-VOD asset ends] に、live-to-VOD アセットの終了日時を入力します。アセットの長さは、エンドポイントのスタートオーバーウィンドウを超えることはできません。エンドポイントのウィンドウが 5 時間であり、開始時間が 2019/07/29 07:15:00 である場合、終了時間を 2019/07/29 12:15:00 より後にすることはできません。終了時間も過去であることが必要です。

## 送信先

送信先情報では、ライブストリームから収集された後の Live-to-VOD アセットを、MediaPackage がどのように保存するかを定義します。

- [IAM ロール ARN] に、live-to-VOD アセットの保存先となる Amazon S3 バケットに対する読み取りおよび書き込みのアクセスを MediaPackage に許可する、IAM ロールの ARN を入力します。これは「[他の AWS サービスへのアクセスを AWS Elemental MediaPackage に許可する](#)」で作成したロールです。

2. [Amazon S3 バケット名] に、MediaPackage が live-to-VOD アセットを保存するバケットの名前を入力します。Amazon S3 バケット名は、MediaPackage が収集するリージョンと同じリージョンにある必要があります。
3. [Manifest key (マニフェストキー)] に、バケット内の Live-to-VOD アセットへのパス (アセットの親マニフェストのファイル名を含む) を入力します。ディレクトリ構造がバケットにまだない場合は、MediaPackage によって作成されます。

#### Important

マニフェストキーは一意であることが必要です。複数の収集ジョブに同じマニフェストキーを使用すると、アセットの最新の再生リストによって既存の再生リストが上書きされます。マニフェストキーを再利用する必要があるのは、コンテンツの前の収集に問題があった場合など、同じコンテンツを収集するときのみです。

## 収集ジョブの詳細の表示

過去 90 日以内に作成したすべての収集ジョブを表示します。90 日後、収集ジョブは期限切れになりアカウントから削除されます。

収集ジョブの表示には、MediaPackage コンソール、AWS CLI、または MediaPackage API を使用します。AWS CLI または MediaPackage API を使用してジョブを表示する方法については、[AWS Elemental MediaPackage API リファレンス](#) を参照してください。

収集ジョブの詳細を表示するには (コンソール)

1. MediaPackage コンソール (<https://console.aws.amazon.com/mediapackage/>) を開きます。
2. ナビゲーションペインの [Live (ライブ)] で、[Harvest jobs (収集ジョブ)] を選択します。
3. [ハーベストジョブ] ページで、ハーベストジョブを選択して詳細を表示します。

## 収集ジョブの編集

収集ジョブを編集することはできません。異なる設定の収集ジョブを作成するには、「[収集ジョブの作成](#)」を参照してください。

## 収集ジョブの削除

収集ジョブを削除することはできません。

- 異なる設定の収集ジョブを作成するには、「[収集ジョブの作成](#)」を参照してください。
- MediaPackage が収集ジョブで作成した VOD アセットを削除するには、Amazon Simple Storage Service Getting 入門ガイドの「[Delete an Object and a Bucket](#)」を参照してください。

# AWS Elemental MediaPackage の機能

次のセクションでは、AWS Elemental MediaPackage で利用可能な機能と仕組みについて説明します。次

## トピック

- [AWS Elemental MediaPackage での CDN 認証](#)
- [AWS Elemental MediaPackage でのコンテンツの暗号化と DRM](#)
- [AWS Elemental MediaPackage の DASH マニフェストオプション](#)
- [マニフェストでのフィルタリング](#)
- [メタデータのパススルー](#)
- [AWS Elemental MediaPackage のレンディショングループのリファレンス](#)
- [AWS Elemental MediaPackage の SCTE-35 メッセージオプション](#)
- [AWS Elemental MediaPackage のタイムシフト表示のリファレンス](#)
- [AWS Elemental MediaPackage でトリックプレイを使用する](#)

## AWS Elemental MediaPackage での CDN 認証

コンテンツ配信ネットワーク (CDN) 認証は、コンテンツを不正使用から保護するのに役立ちます。CDN 認証を設定すると、は MediaPackage と CDN の間で承認された再生リクエスト MediaPackage のみを実行します。これにより、ユーザーがオリジン上のコンテンツに直接アクセスするために CDN をバイパスするのを防ぐことができます。

## 仕組み

へのコンテンツリクエストにカスタム HTTP ヘッダーを含める CloudFront ように、Amazon などの CDN を設定します MediaPackage。

カスタム HTTP ヘッダーと値の例。

```
X-MediaPackage-CDNIdentifier: 9ceebbe7-9607-4552-8764-876e47032660
```

ヘッダー値を、シークレットとして AWS Secrets Manager に保存します。CDN が再生リクエストを送信すると、MediaPackage はシークレットの値がカスタム HTTP ヘッダー値と一致する

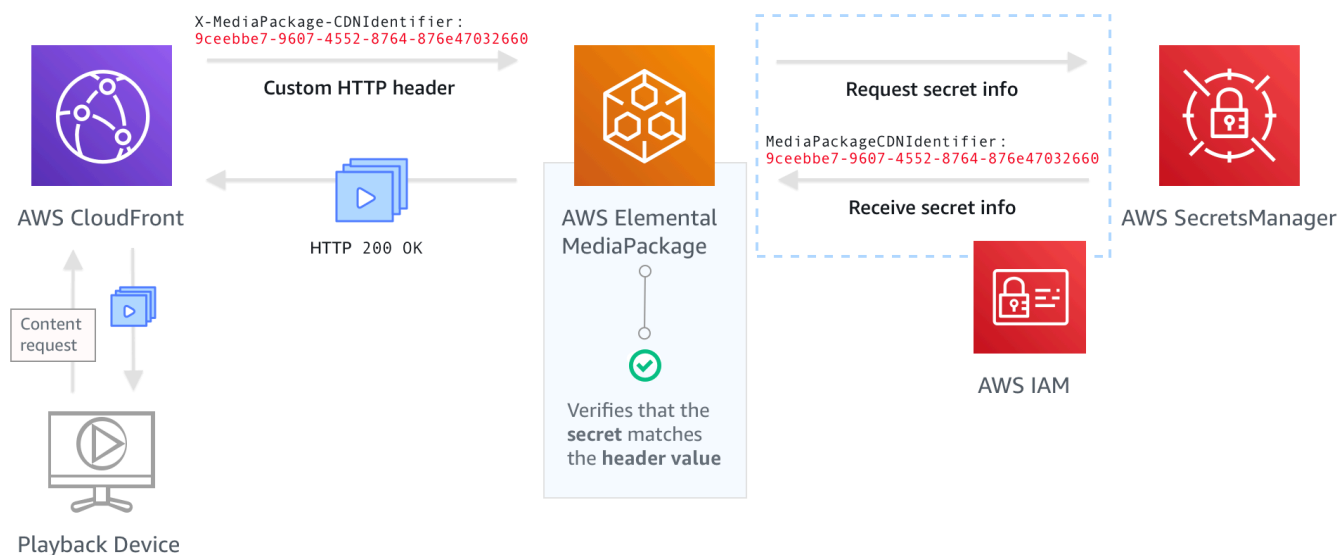
MediaPackage ことを確認します。には、アクセス許可ポリシーとロールを使用してシークレットを読み取るAWS Identity and Access Managementアクセス許可が付与されます。

シークレットキーと値の例。

```
{"MediaPackageCDNIdentifier": "9ceebbe7-9607-4552-8764-876e47032660"}
```

値が一致すると、は HTTP 200 OKステータスコードとともにコンテンツ MediaPackage を保存します。一致しない場合、または認証リクエストが失敗した場合、MediaPackage はコンテンツを供給せず、HTTP 403 Unauthorizedステータスコードを送信します。

次の図は、Amazon を使用した正常な CDN 認証を示しています CloudFront。



CDN 認証を設定する方法については、step-by-step 「」を参照してください [CDN 認証の設定](#)。

## CDN 認証の設定

CDN 認証を設定するには、次のステップを完了します。

### トピック

- [ステップ 1: CDN カスタムオリジン HTTP ヘッダーを設定する](#)
- [ステップ 2: 値をシークレットとして AWS Secrets Manager に保存します。](#)

- [ステップ 3: Secrets Manager MediaPackage にアクセスするための IAM ポリシーとロールを作成する](#)
- [ステップ 4: で CDN 認証を有効にする MediaPackage](#)

## ステップ 1: CDN カスタムオリジン HTTP ヘッダーを設定する

CDN で、ヘッダー **X-MediaPackage-CDNIdentifier** と値を含むカスタムオリジン HTTP ヘッダーを設定します。値には、36 文字の文字列を生成する [UUID バージョン 4](#) 形式を使用することをお勧めします。UUID バージョン 4 形式を使用していない場合、値を 8~128 文字にする必要があります。

### Important

選択する値は静的な値である必要があります。CDN と AWS Secrets Manager の間にはネイティブ統合がないので、値は CDN と AWS Secrets Manager の両方で静的にする必要があります。CDN とシークレットを設定した後、この値を変更する場合は、手動で値を更新する必要があります。詳細については、「[CDN ヘッダー値の更新](#)」を参照してください。

### ヘッダーと値の例

```
X-MediaPackage-CDNIdentifier: 9ceebbe7-9607-4552-8764-876e47032660
```

Amazon でカスタムヘッダーを作成するには CloudFront

1. にサインインAWS Management Consoleし、 で CloudFront コンソールを開きます<https://console.aws.amazon.com/cloudfront/v4/home>。
2. ディストリビューションを作成または編集します。
3. [オリジンの設定] で、フィールドに入力します。この同じ値を、Secrets Manager のシークレットにも使用します。
  - [ヘッダー名] に **X-MediaPackage-CDNIdentifier** と入力します。
  - [値] に値を入力します。36 文字の文字列を生成する UUID バージョン 4 形式を使用することをお勧めします。UUID バージョン 4 形式を使用していない場合、値を 8~128 文字にする必要があります。
4. 残りのフィールドに入力し、ディストリビューションを保存します。

のカスタムヘッダーの詳細については CloudFront、「Amazon CloudFront デベロッパーガイド」の「[オリジンへの顧客ヘッダーの転送](#)」を参照してください。

## ステップ 2: 値をシークレットとして AWS Secrets Manager に保存します。

AWS Secrets Manager のシークレットとしてカスタムオリジンの HTTP ヘッダーに使用したものと、同じ値を保存します。シークレットには、AWS Elemental MediaPackage リソースと同じ AWS アカウントとリージョン設定を使用する必要があります。MediaPackage は、アカウントまたはリージョン間でのシークレットの共有をサポートしていません。ただし、同じリージョン内および同じアカウントの複数のエンドポイントで同じシークレットを使用することはできます。

Secrets Manager にシークレットを保存するには

1. 次の場所で AWS Secrets Manager コンソールにサインインします: <https://console.aws.amazon.com/secretsmanager/>。
2. [新しいシークレットの保存] を選択します。[シークレットのタイプ] で、[その他のシークレットのタイプ] を選択します。
3. [キー/値のペア] に、キーと値の情報を入力します。
  - 左側のボックスに **MediaPackageCDNIdentifier** を入力します。
  - 右側のボックスに、カスタムオリジン HTTP ヘッダーに設定した値を入力します。例えば、「9ceebbe7-9607-4552-8764-876e47032660」と入力します。
4. 暗号化キー の場合、デフォルト値を のままにしておくことができますDefaultEncryptionKey。
5. [次へ] をクリックします。
6. [シークレットの名前] には、MediaPackage で使用するシークレットであることがわかるように、プレフィックス **MediaPackage/** を付けることをお勧めします。例えば、「**MediaPackage/cdn\_auth\_us-west-2**」と入力します。
7. [次へ] をクリックします。
8. [自動ローテーションを設定する] は、既定の [自動ローテーションを無効にする] 設定のままにします。

認証コードを後でローテーションする必要がある場合は、「[CDN ヘッダー値の更新](#)」を参照してください。
9. [Next] (次へ) を選択してから、[Store] (保存) を選択します。

これにより、シークレットのリストに移動します。



- シークレット名を選択して、[シークレットの ARN] を表示します。ARN は、`arn:aws:secretsmanager:us-west-2:123456789012:secret:MediaPackage/cdn_auth_test-xxxxxx` のような値です。シークレット ARN は、「ステップ 4: MediaPackage で CDN 認証を有効にする」で、MediaPackage の CDN 認証を設定するときに使用します。

### ステップ 3: Secrets Manager MediaPackage にアクセスするための IAM ポリシーとロールを作成する

Secrets Manager への MediaPackage 読み取りアクセスを許可する IAM ポリシーとロールを作成します。MediaPackage は CDN から再生リクエストを受信すると、保存されているシークレット値がカスタム HTTP ヘッダーの値と一致することを確認します。[the section called “他の AWS サービスへのアクセスを AWS Elemental MediaPackage に許可する”](#) のステップに従って、ポリシーとロールを設定します。

### ステップ 4: で CDN 認証を有効にする MediaPackage

MediaPackage コンソール、AWS CLI または MediaPackage API を使用して、エンドポイントまたはビデオオンデマンド (VOD) パッケージグループの CDN 認証を有効にできます。ステップ 3: Secrets Manager MediaPackage にアクセスするための IAM ポリシーとロールを作成するで作成する IAM ポリシーとロールには ARN を使用します。

#### Tip

同じリージョン内および同じアカウントの複数のエンドポイントでは、同じシークレットを使用します。ワークフローに必要な場合にのみ、新しいシークレットを作成することで、コストを削減します。

コンソールを使用してライブコンテンツの CDN 認証を有効にするには

- <https://console.aws.amazon.com/mediapackage/> で MediaPackage コンソールを開きます。
- チャンネルがまだない場合は、チャンネルを作成します。ヘルプについては、「[チャンネルの作成](#)」を参照してください。
- エンドポイントを作成または編集します。
- [アクセスコントロールの設定] で、[CDN 認証の使用] を選択します。フィールドに入力します。

- [シークレットロール ARN] に、「[ステップ 3: Secrets Manager MediaPackage にアクセスするための IAM ポリシーとロールを作成する](#)」で作成した IAM ロールの ARN を入力します。
  - [CDN 識別子シークレット ARN] に、CDN がエンドポイントへのアクセス認証に使用する Secrets Manager でのシークレットの ARN を入力します。
5. 必要に応じて残りのフィールドに入力し、エンドポイントを保存します。

コンソールを使用して VOD コンテンツの CDN 認証を有効にするには

1. <https://console.aws.amazon.com/mediapackage/> で MediaPackage コンソールを開きます。
2. VOD パッケージンググループをまだ作成していない場合は、作成します。ヘルプについては、「[パッケージンググループの作成](#)」を参照してください。
3. パッケージンググループを作成または編集します。
4. [アクセスコントロールを設定] で、[認証を有効にする] を選択します。フィールドに入力します。
  - [シークレットロール ARN] に、「[ステップ 3: Secrets Manager MediaPackage にアクセスするための IAM ポリシーとロールを作成する](#)」で作成した IAM ロールの ARN を入力します。
  - [CDN 識別子シークレット ARN] に、CDN がエンドポイントへのアクセス認証に使用する Secrets Manager でのシークレットの ARN を入力します。
5. 必要に応じて残りのフィールドに入力し、パッケージンググループを保存します。

これで、CDN 認証のセットアップが完了しました。このエンドポイントへのリクエストには、Secrets Manager に保存したものと同一認証コードが含まれている必要があります。

MediaPackage API で CDN 認証を有効にするには

MediaPackage API で CDN 認証を有効にする方法については、以下の API リファレンスを参照してください。

- [MediaPackage ライブ API リファレンス](#)
- [MediaPackage VOD API リファレンス](#)

## CDN ヘッダー値の更新

CDN カスタムオリジン HTTP ヘッダーの値を変更する場合は、Secrets Manager に保存されているシークレット値を更新する必要があります。次の手順では、Secrets Manager 内の値を更新して、CDN の HTTP ヘッダー値と Secrets Manager に保存されているシークレット値が、同期していることを確認する方法について説明します。

値を更新するには

1. AWS Secrets Manager ユーザーガイドの「[シークレットの変更](#)」にある説明に従って、Secrets Manager に格納されたシークレット値を更新します。

アクティブなストリームの再生が継続されるように、は Secrets Manager の現在の値を使用するか、1つのバージョンを戻すリクエスト MediaPackage を承認します。

2. Secrets Manager で値が変更されたことを が認識 MediaPackage するまで 10 分待ちます。
3. CDN で、X-MediaPackage-CDNIdentifier の値を新しい認証コードに更新します。
4. CDN が新しい値で完全に更新されるのを待ってから、この CDN 経由でリクエストを MediaPackage に送信します。

前のシークレット値を無効にするには、新しいシークレット値を 2 回保存します。こうすることで、現在のシークレットバージョンと以前のシークレットバージョンの両方が同じ値を持ちます。

## AWS Elemental MediaPackage でのコンテンツの暗号化と DRM

コンテンツ暗号化とデジタル著作権管理 (DRM) によって、コンテンツを不正使用から保護します。AWS Elemental MediaPackage は [AWS Secure Packager and Encoder Key Exchange \(SPEKE\) API](#) を使用して、DRM プロバイダーによるコンテンツの暗号化と復号化を容易にします。SPEKE を使用すると、DRM プロバイダーは SPEKE API MediaPackage を通じて暗号化キーを に提供します。同時に DRM プロバイダーは、サポートしているメディアプレイヤー用に復号化のためのライセンスも提供します。クラウドで実行されているサービスや機能での SPEKE の使用については、Secure Packager and Encoder Key Exchange API Specification guide の「[AWS cloud-based architecture](#)」を参照してください。

### 制限事項と要件

AWS Elemental MediaPackage のコンテンツ暗号化を実装する場合は、以下の制限事項と要件を参照してください。

- デジタル著作権管理 (DRM) プロバイダーとの統合を容易にする、AWS Secure Packager and Encoder Key Exchange (SPEKE) API を使用します。SPEKE の詳細については、「[What is Secure Packager and Encoder Key Exchange?](#)」を参照してください。
- 使用する DRM プロバイダーで、SPEKE がサポートされている必要があります。SPEKE をサポートする DRM プロバイダーのリストについては、「MediaPackage ユーザーガイド」の「[DRM プラットフォームプロバイダーでオンボードする](#)」トピックを参照してください。DRM ソリューションプロバイダーは、で DRM 暗号化の使用を設定するのに役立ちます MediaPackage。
- を使用して MediaPackage、ライブおよびビデオオンデマンド (VOD) コンテンツを暗号化します。MediaPackage VOD サービスを通じて配信する必要があるアセットは、暗号化されていない HLS ライブエンドポイントから収集する必要があります。DRM または暗号化で保護されている HLS および DASH のエンドポイントから live-to-VOD アセットを収集できます。ただし、MediaPackage VOD サービスは暗号化された (明確ではない) コンテンツであるため、これらのアセットを取り込むことはできません。この種類のワークフローの詳細については、「[AWS Elemental MediaPackage を使用した live-to-VOD アセットの作成](#)」を参照してください。

以下のセクションでは、の SPEKE を使用してコンテンツ暗号化を選択および実装する方法に関するガイダンスを提供します MediaPackage。

## トピック

- [適切な SPEKE バージョンを選択する](#)
- [SPEKE のデプロイ](#)
- [コンテンツキーで使用する証明書の準備と管理](#)
- [キーローテーションの動作について](#)
- [SPEKE バージョン 2.0 のプリセット](#)

## 適切な SPEKE バージョンを選択する

[SPEKE バージョン 1](#) は、[CPIX バージョン 2.0](#) を使用して、すべてのオーディオトラックと動画トラックでの単一の暗号化キーの使用をサポートします。[SPEKE バージョン 2.0](#) は、[CPIX バージョン 2.3](#) を使用して、オーディオトラックと動画トラックでの複数の異なる暗号化キーの使用をサポートします。SPEKE バージョン 2.0 の暗号化設定の詳細については、「[SPEKE バージョン 2.0 のプリセット](#)」を参照してください。

複数のキー暗号化または Content Protection Information Exchange (CPIX) バージョン 2.3 の使用がコンテンツ配信の必須要件である場合は、SPEKE バージョン 2.0 の使用をお勧めします。ただし、SPEKE バージョン 2.0 のサポートは、のエンドポイントタイプ間でプログレッシブです MediaPackage。そのため、キーローテーションなど、一部のライブオプションはまだ利用できません。SPEKE の統合戦略を計画する際には、これらの制約事項を考慮してください。の SPEKE バージョン 2.0 ロードマップの詳細については MediaPackage、AWS アカウント チームにお問い合わせください。

## サポートされているプロトコルと DRM プラットフォーム

以下の表に、SPEKE バージョン 1.0 および SPEKE バージョン 2.0 でサポートされる各種のプロトコルとデジタル著作権管理 (DRM) プラットフォームを示します。

### Note

Irdeeto のコンテンツ保護は SPEKE バージョン 1.0 との組み合わせではサポートされていません。

SPEKE バージョン 1.0 – プロトコルと DRM システムのサポート一覧表	Microsoft PlayReady	Google Widevine	Apple FairPlay	AES-128
ライブ				
Apple HLS	Not supported	Not supported	✓ キーローテーションあり	✓ キーローテーションあり
CMAF Apple HLS	Not supported	✓ キーローテーションあり  cbcs 暗号化のみをサポート	✓ キーローテーションあり  cbcs 暗号化のみをサポート	Not supported

DASH	√	√	Not supported	Not supported
	キーローテーションあり	キーローテーションあり		
Microsoft Smooth	√	Not supported	Not supported	Not supported
VOD				
Apple HLS	Not supported	Not supported	√	√
CMAF Apple HLS	Not supported	√	√	Not supported
		cbcs 暗号化のみをサポート	cbcs 暗号化のみをサポート	
DASH	√	√	Not supported	Not supported
Microsoft Smooth	√	Not supported	Not supported	Not supported
SPEKE バージョン 2.0 – プロトコルと DRM システムのサポート一覧表	Microsoft PlayReady	Google Widevine	Apple FairPlay	Irdeto のコンテンツ保護
ライブ				
CMAF Apple HLS	√	√	√	Not supported
	cbcs 暗号化と cenc 暗号化をサポート	cbcs 暗号化と cenc 暗号化をサポート	cbcs 暗号化をサポート	
DASH	√	√	Not supported	√
VOD				

CMAF Apple HLS	√	√	√	Not supported
	cbcs 暗号化のみをサポート	cbcs 暗号化のみをサポート	cbcs 暗号化のみをサポート	
DASH	√	√	Not supported	√

## SPEKE のデプロイ

デジタル著作権管理 (DRM) ソリューションプロバイダーは、で DRM 暗号化を使用するためのセットアップに役立ちます MediaPackage。通常、プロバイダーは、AWS リージョン MediaPackage が実行されているのと同じ AWS アカウントの にデプロイする SPEKE ゲートウェイを提供します。適切な暗号化設定でオリジンエンドポイントを設定することに加えて、MediaPackage がイベントとして生成している [キープロバイダーイベントのイベント通知を設定](#) する必要があります CloudWatch。エンドポイントに暗号化を設定する方法については、プロトコルに対応したセクションを参照してください: [HLS 暗号化フィールド](#)、[MSS 暗号化フィールド](#)、[CMAF 暗号化フィールド](#)、[DASH 暗号化フィールド](#)。

キーサービス MediaPackage に接続するために独自の API Gateway を構築する必要がある場合は、で利用可能な [SPEKE リファレンスサーバー](#) を開始点 GitHub として使用できます。

## コンテンツキーで使用する証明書の準備と管理

AWS Elemental MediaPackage は、Content Protection Information Exchange (CPIX) ドキュメントを使用して、コンテンツの暗号化に使用されるコンテンツキーに関する通信を SPEKE との間で行います。最も安全なデジタル著作権管理 (DRM) 暗号化ソリューションでは、CPIX ドキュメントで暗号化されたコンテンツキーを使用します。

暗号化されたコンテンツキーを使用するには、次の要件を満たす必要があります。

- 暗号化されたコンテンツはライブである必要があります。ビデオオンデマンド (VOD) ワークフローおよび Live-to-VOD ワークフローでは、CPIX ドキュメント内の暗号化されたコンテンツキーはサポートされません。
- DRM キープロバイダーは、暗号化されたコンテンツキーをサポートする必要があります。コンテンツキーの暗号化を扱えないキープロバイダーに対してこの機能を有効にした場合、再生は失敗します。



- を実行するのと同じリージョンの AWS Certificate Manager (ACM) に適切な証明書をインポートする必要があります MediaPackage。ACM の詳細については、「[AWS Certificate Manager ユーザーガイド](#)」を参照してください。

次の手順では、証明書を準備および管理する方法について説明します。

DRM コンテンツキー暗号化の証明書を準備するには

1. 2048 RSA、SHA-512 署名証明書を取得します。
2. ACM コンソール (<https://console.aws.amazon.com/acm/>) を開きます。
3. 「[AWS Certificate Manager に証明書をインポートする。](#)」の手順に従って、証明書を ACM にインポートします。後で必要になるので、その結果の証明書 ARN を書き留めておきます。

DRM 暗号化で使用する証明書では、ACM でのステータスが [Issued] (発行済み) となっている必要があります

証明書を AWS Elemental MediaPackage で使用するには

エンドポイント設定で DRM 暗号化を使用する場合、暗号化パラメータで証明書 ARN を提供します。これにより、コンテンツキーを暗号化します。複数のイベントに対して同じ証明書 ARN を使用できます。詳細については、[the section called “エンドポイントの使用”](#) で暗号化設定情報を参照してください。

証明書を更新するには

AWS Elemental MediaPackage で使用している証明書を更新するには、ACM で再インポートします。証明書は、MediaPackage での使用を中断することなく更新されます。

証明書を削除するには

ACM から証明書を削除するには、その他のサービスと関連付けられていない状態である必要があります。使用しているエンドポイント設定から証明書 ARN を削除してから、ACM から削除します。

#### Note

アクティブなエンドポイントから証明書 ARN を削除した場合、エンドポイントは実行され続けますが、コンテンツキーの暗号化の使用は停止されます。

## キーローテーションの動作について

HLS、CMAF、および DASH のエンドポイントからライブコンテンツのキーローテーションを有効にすると、AWS Elemental MediaPackage はライブコンテンツの開始前にコンテンツキーを取得します。MediaPackage「」で説明されているように、コンテンツが進行すると、はエンドポイントに設定した間隔で新しいキーを取得します [パッケージの暗号化フィールド](#)。

MediaPackage がコンテンツキーを取得できない場合、次のアクションを実行します。

- 以前にこのエンドポイントのコンテンツキーを MediaPackage 正常に取得した場合、最後に取得したキーが使用されます。これにより、以前に動作したエンドポイントが引き続き動作します。
- MediaPackage が以前にこのエンドポイントのコンテンツキーを正常に取得しなかった場合、は再生リクエストにエラー 404 で MediaPackage 応答します。

いずれの場合も、MediaPackage がコンテンツキーを取得できない場合、で説明されているように、CloudWatch イベントが生成されます [キープロバイダーの通知イベント](#)。

## SPEKE バージョン 2.0 のプリセット

SPEKE バージョン 2.0 では、オーディオトラックとビデオトラックに複数の異なる暗号化キーを使用して暗号化 MediaPackage を設定できます。MediaPackage API はこれらのプリセットを定義し、パッケージ暗号化エンドポイント設定セクションのビデオ暗号化プリセットとオーディオ暗号化プリセットメニューの MediaPackage コンソールに表示されます。プリセットは、オーディオトラックのチャンネル数、ビデオトラックのビデオ解像度に基づいて、暗号化キーを特定のオーディオトラックまたはビデオトラックにマッピングします。は、オーディオとビデオの暗号化プリセットの特定の組み合わせ MediaPackage を使用して、次の 3 つの異なる暗号化シナリオをサポートします。

- [シナリオ 1: 暗号化されないトラックと暗号化されるトラック](#)
- [シナリオ 2: すべてのオーディオトラックと動画トラックでの単一の暗号化キー](#)
- [シナリオ 3: オーディオトラックと動画トラックでの複数の暗号化キー](#)

### シナリオ 1: 暗号化されないトラックと暗号化されるトラック

[動画暗号プリセット] または [オーディオ暗号プリセット] メニューで [UNENCRYPTED] プリセットを選択すると、オーディオトラックまたは動画トラックを暗号化しないようにできます。オーディオと動画のプリセットの両方に [UNENCRYPTED] を選択することはできません。どのトラックも暗号

化するつもりはないということになるためです。また、[SHARED] は特別なプリセットであるため、オーディオおよび動画に [UNENCRYPTED] プリセットと [SHARED] プリセットを組み合わせることはできません。詳細については、「[シナリオ 2: すべてのオーディオトラックと動画トラックでの単一の暗号化キー](#)」を参照してください。

[UNENCRYPTED] プリセットの有効な組み合わせを以下に示します。

- オーディオトラックでの [UNENCRYPTED] と名前が PRESET-VIDEO- で始まる動画プリセット
- 動画トラックでの [UNENCRYPTED] と名前が PRESET-AUDIO- で始まるオーディオプリセット

## シナリオ 2: すべてのオーディオトラックと動画トラックでの単一の暗号化キー

SPEKE バージョン 2.0 の [SHARED] プリセットは、SPEKE バージョン 1.0 と同様に、すべてのオーディオおよび動画トラックに 1 つの暗号化キーを使用します。[SHARED] プリセットを選択する場合は、オーディオと動画の両方の暗号化に使用するよう選択します。

## シナリオ 3: オーディオトラックと動画トラックでの複数の暗号化キー

PRESET-VIDEO- または で始まる名前のプリセットを使用すると PRESET-AUDIO-、 は特定のプリセットが定義する暗号化キーの数でオーディオトラックとビデオトラックを MediaPackage 暗号化します。次の表は、キーサーバーからのキー MediaPackage リクエストの数と、それらのキーが追跡にどのようにマッピングされるかを示しています。特定のキーの基準に一致するトラックがない場合、MediaPackage はそのキーを使用してトラックを暗号化しません。

MediaPackage は、解像度に対応するキーを使用して、1 フレームのみのトリックプレートトラックを暗号化します。

次の表では、キー名の値は、CPIX ドキュメントで が MediaPackage 使用する ContentKeyUsageRule@IntendedTrackType 属性の値です。この値は、特定のコンテンツキーの SPEKE サーバーに送信されます。

### 動画暗号化のプリセット

プリセット名	キーの数	キー名	最小解像度	最大解像度
PRESET-VIDEO-1	1	VIDEO	最小または最大解像度はありません。はすべてのトラックを同じキーで MediaPackage 暗号化します。	

プリセット名	キーの数	キー名	最小解像度	最大解像度
PRESET-VIDEO-2	2	SD	最小解像度なし	<= 1024x576
		HD	> 1024x576	最大解像度なし
PRESET-VIDEO-3	3	SD	最小解像度なし	<= 1024x576
		HD	> 1024x576	<= 1920x1080
		UHD	> 1920x1080	最大解像度なし
PRESET-VIDEO-4	4	SD	最小解像度なし	<= 1024x576
		HD	> 1024x576	<= 1920x1080
		UHD1	> 1920x1080	<= 4096x2160
		UHD2	> 4096x2160	最大解像度なし
PRESET-VIDEO-5	5	SD	最小解像度なし	<= 1024x576
		HD1	> 1024x576	<= 1280x720
		HD2	> 1280x720	<= 1920x1080
		UHD1	> 1920x1080	<= 4096x2160
		UHD2	> 4096x2160	最大解像度なし
PRESET-VIDEO-6	4	SD	最小解像度なし	<= 1024x576
		HD1	> 1024x576	<= 1280x720
		HD2	> 1280x720	<= 1920x1080
		UHD	> 1920x1080	最大解像度なし
PRESET-VIDEO-7	3	SD+HD1	最小解像度なし	<= 1280x720
		HD2	> 1280x720	<= 1920x1080

プリセット名	キーの数	キー名	最小解像度	最大解像度
		UHD	> 1920x1080	最大解像度なし
PRESET-VIDEO-8	4	SD+HD1	最小解像度なし	<= 1280x720
		HD2	> 1280x720	<= 1920x1080
		UHD1	> 1920x1080	<= 4096x2160
		UHD2	> 4096x2160	最大解像度なし
SHARED	1	すべて	最小解像度または最大解像度はありません。は、すべてのビデオトラックとオーディオトラックを同じキーで MediaPackage 暗号化します。	
UNENCRYPTED	0	該当なし	MediaPackage はビデオトラックを暗号化しません。	

次の表では、キー名の値は、CPIX ドキュメントで が MediaPackage 使用する ContentKeyUsageRule@IntendedTrackType 属性の値です。この値は、特定のコンテンツキーの SPEKE サーバーに送信されます。

#### オーディオ暗号化プリセット

プリセット名	キーの数	キー名	最小チャンネル数	最大チャンネル数
PRESET-AUDIO-1	1	AUDIO	チャンネルの最小数または最大数はありません。MediaPackage は、すべてのオーディオトラックとビデオトラックを同じキーで暗号化します。	
PRESET-AUDIO-2	2	STEREO_AUDIO	最小解像度なし	2
		MULTICHANNEL_AUDIO	> 2	最大解像度なし

プリセット名	キーの数	キー名	最小チャンネル数	最大チャンネル数
PRESET-AUDIO-3	3	STEREO_AUDIO	最小解像度なし	2
		MULTICHANNEL_AUDIO_3_6	> 2	<= 6
		MULTICHANNEL_AUDIO_7	> 6	最大解像度なし
SHARED	1	すべて	チャンネルの最小数または最大数はありません。MediaPackage は、すべてのオーディオトラックとビデオトラックを同じキーで暗号化します。	
UNENCRYPTED	0	該当なし	MediaPackage はオーディオトラックを暗号化しません。	

これで、が暗号化されていないトラックと暗号化されたトラックに対して SPEKE バージョン 2.0 プリセット MediaPackage をサポートする方法がわかりました。これらのプリセットを使用すると、すべてのオーディオトラックと動画トラックで単一の暗号化キーを使用したり、オーディオトラックと動画トラックで複数の暗号化キーを使用したりできます。

## AWS Elemental MediaPackage の DASH マニフェストオプション

このセクションでは、ライブ出力 DASH マニフェストを変更するために AWS Elemental MediaPackage に用意されているオプションについて説明します。

これらのオプションは、ビデオオンデマンド (VOD) 出力または収集された Live-to-VOD アセットには適用されません。

デフォルトの DASH マニフェスト

以下に示すのは、処理されずに切り捨てられた DASH マニフェストの例です。

```
<MPD>
  <Period>
```

```
<AdaptationSet>
  <Representation>
    <SegmentTemplate>
      <SegmentTimeline>
        <S />
      </SegmentTimeline>
    </SegmentTemplate>
  </Representation>
</AdaptationSet>
.
.
</Period>
</MPD>
```

DASH マニフェストの要素は、MPD (メディア表現の説明) オブジェクト内にネストされます。マニフェストの要素には次のものがあります。

- **Period** - マニフェスト全体が 1 期間内にネストされます。
- **AdaptationSet** - 同じタイプの表現 (動画、オーディオ、キャプション) をまとめます。Period には 1 つ以上の AdaptationSets があります。
- **Representation** - オーディオ、動画、キャプショントラックについて説明します。各 AdaptationSet には 1 つ以上の Representations があります。各表現はトラックです。
- **SegmentTemplate** - メディアおよび初期化セグメントのタイムスケールやアクセス URL など、表現のプロパティを定義します。各 Representation に対して 1 つの SegmentTemplate があります。
- **SegmentTimeline** - 各セグメントでいつ再生が可能になるかを説明します。各 SegmentTemplate に対して 1 つの SegmentTimeline があります。
- **S** - セグメントがいつ利用可能になるか (t の値)、セグメントの長さ (d の値)、長さが同じ追加の連続セグメントの数 (r の値) を説明します。SegmentTimeline には 1 つ以上のセグメントがあります。

MediaPackage では、これらの要素の一部がどのように出力マニフェストに記載されるかを変更できます。出力ライブマニフェストでは、以下の処理オプションを使用できます。

- マニフェストを複数の期間に分割して、広告時間枠を許可する。「[AWS Elemental MediaPackage の DASH マニフェストオプション](#)」を参照してください。
- マニフェストの長さを減らし、処理と再生をより効率化する。「[圧縮された DASH マニフェスト](#)」を参照してください。



- メディア URL 情報で使われるセグメント情報を、SegmentTemplate プロパティで管理する。  
「[DASH マニフェストのセグメントテンプレート形式](#)」を参照してください。

## AWS Elemental MediaPackage の複数期間 DASH

AWS Elemental MediaPackage では、VOD とライブの両方で DASH マニフェストに複数期間を挿入できます。

期間とは、DASH マニフェストのコンテンツのひとかたまりであり、開始時間と再生時間で定義されます。マニフェストのデフォルトでは、その全体が 1 つの期間に含まれます。MediaPackage では、DASH マニフェストを複数の期間に分けることで、広告とメインコンテンツ間の境界を指定できます。例えば、AWS Elemental MediaTailor のようなダウンストリーム広告サービスを含む MediaPackage を使用している場合は、MediaPackage の MPEG-DASH エンドポイントで、[Trigger new period on ads] を選択します。このオプションにより、DASH マニフェストが複数の期間でフォーマットされる必要があることを MediaPackage に指示します。

- AWS Elemental MediaTailor の詳細については、[AWS Elemental MediaTailor ユーザーガイド](#)を参照してください。
- MediaPackage の DASH-ISO エンドポイントの詳細については、「[DASH エンドポイントの作成](#)」を参照してください。
- MediaPackage での複数期間の DASH の動作については、以下の仕組みに関するセクションを参照してください。

### 複数期間 DASH の仕組み

複数期間の DASH の機能を使用するには、SCTE-35 広告マーカーマッセージを MediaPackage への入力に含める必要があります。これらのメッセージにより、MediaPackage に期間の境界を作成するポイントを通知します。MediaPackage でそれらのメッセージを処理する方法は次のとおりです。

1. MediaPackage が入力ソースから SCTE-35 のメッセージを検出します。
2. MediaPackage は、SCTE-35 メッセージの属性を使用して、メインコンテンツの最後と広告の間のどの部分に境界があるかを計算します。この計算式は  $(\text{scte35 ptsAdjustment} + \text{scte35 ptsTime}) / (\text{EventStream timescale})$  となります。

## Example

次の例では、44.075 秒の時点で期間が開始されています。これは、 $(183003 + 3783780) / 90000 = 44.075$  となるためです。

```
<Period start="PT44.075S" id="21">
  <EventStream timescale="90000" schemeIdUri="urn:scte:scte35:2013:xml">
    <Event>
      <scte35:SpliceInfoSection protocolVersion="0" ptsAdjustment="183003"
tier="4095">
        <scte35:SpliceInsert spliceEventId="1000"
spliceEventCancelIndicator="false" outOfNetworkIndicator="true"
spliceImmediateFlag="false" uniqueProgramId="7" availNum="1" availsExpected="4">
          <scte35:Program><scte35:SpliceTime ptsTime="3783780"/></scte35:Program>
        </scte35:SpliceInsert>
      </scte35:SpliceInfoSection>
    </Event>
  </EventStream>
  .
  .
</Period>
```

- MediaPackage は EventStream と Event、ならびに追加情報を伴う scte35 タグをマニフェストに挿入します。さらに先の例のように、Period タグを使用して広告期間を囲みます。最初の広告が期間に入る前に MediaPackage によりすべての適応セットがグループ化されます。また、後続の適応セットは、続く SCTE-35 マーカーまでに対応する期間内でグループ化されます。複数期間を使用したマニフェストの完全な例を次に示します。SpliceInsertSCTE-35 広告マーカーを使用します。

## Example

```
<?xml version="1.0" encoding="utf-8"?>
<MPD>
  <Period start="PT0.000S" id="0" duration="PT44.075S">
    <AdaptationSet mimeType="video/mp4" segmentAlignment="true"
subsegmentAlignment="true" startWithSAP="1" subsegmentStartsWithSAP="1"
bitstreamSwitching="true">
      <Representation id="1" width="960" height="540" frameRate="30000/1001"
bandwidth="1000000" codecs="avc1.4D401F">
```

```

    <SegmentTemplate timescale="30000" media="index_video_1_0_${Number$.mp4?
m=1528413503" initialization="index_video_1_0_init.mp4?m=1528413503" startNumber="6"
presentationTimeOffset="0">
      <SegmentTimeline>
        <S t="361301" d="60060" r="15"/>
      </SegmentTimeline>
    </SegmentTemplate>
  </Representation>
</AdaptationSet>
<AdaptationSet mimeType="audio/mp4" segmentAlignment="0" lang="eng">
  <Representation id="2" bandwidth="96964" audioSamplingRate="48000"
codecs="mp4a.40.2">
    <SegmentTemplate timescale="48000" media="index_audio_2_0_${Number$.mp4?
m=1528413503" initialization="index_audio_2_0_init.mp4?m=1528413503" startNumber="6"
presentationTimeOffset="0">
      <SegmentTimeline>
        <S t="578305" d="96256" r="3"/>
        <S t="963329" d="95232"/>
        <S t="1058561" d="96256" r="5"/>
        <S t="1636097" d="95232"/>
        <S t="1731329" d="96256" r="3"/>
      </SegmentTimeline>
    </SegmentTemplate>
  </Representation>
</AdaptationSet>
</Period>
<Period start="PT44.075S" id="21">
  <EventStream timescale="90000" schemeIdUri="urn:scte:scte35:2013:xml">
    <Event>
      <scte35:SpliceInfoSection protocolVersion="0" ptsAdjustment="183003"
tier="4095">
        <scte35:SpliceInsert spliceEventId="1000"
spliceEventCancelIndicator="false" outOfNetworkIndicator="true"
spliceImmediateFlag="false" uniqueProgramId="7" availNum="1" availsExpected="4">
          <scte35:Program><scte35:SpliceTime ptsTime="3783780"/></scte35:Program>
        </scte35:SpliceInsert>
      </scte35:SpliceInfoSection>
    </Event>
  </EventStream>
  <AdaptationSet mimeType="video/mp4" segmentAlignment="true"
subsegmentAlignment="true" startWithSAP="1" subsegmentStartsWithSAP="1"
bitstreamSwitching="true">
    <Representation id="1" width="960" height="540" frameRate="30000/1001"
bandwidth="1000000" codecs="avc1.4D401F">

```

```

    <SegmentTemplate timescale="30000" media="index_video_1_0_${Number}.mp4?
m=1528413503" initialization="index_video_1_0_init.mp4?m=1528413503" startNumber="22"
presentationTimeOffset="1322261">
      <SegmentTimeline>
        <S t="1322261" d="60060" r="13"/>
      </SegmentTimeline>
    </SegmentTemplate>
  </Representation>
</AdaptationSet>
<AdaptationSet mimeType="audio/mp4" segmentAlignment="0" lang="eng">
  <Representation id="2" bandwidth="96964" audioSamplingRate="48000"
codecs="mp4a.40.2">
    <SegmentTemplate timescale="48000" media="index_audio_2_0_${Number}.mp4?
m=1528413503" initialization="index_audio_2_0_init.mp4?m=1528413503" startNumber="22"
presentationTimeOffset="2115617">
      <SegmentTimeline>
        <S t="2116353" d="96256"/>
        <S t="2212609" d="95232"/>
        <S t="2307841" d="96256" r="5"/>
        <S t="2885377" d="95232"/>
        <S t="2980609" d="96256" r="4"/>
      </SegmentTimeline>
    </SegmentTemplate>
  </Representation>
</AdaptationSet>
</Period>
</MPD>

```

TimeSignal の代わりに SpliceInsert SCTE-35 広告マーカーを入力内容に含む場合、広告期間の EventStream は次のようになります。

```

<EventStream timescale="90000" schemeIdUri="urn:scte:scte35:2013:xml">
  <Event>
    <scte35:SpliceInfoSection protocolVersion="0" ptsAdjustment="183265" tier="4095">
      <scte35:TimeSignal>
        <scte35:SpliceTime ptsTime="1350000"/>
      </scte35:TimeSignal>
      <scte35:SegmentationDescriptor segmentationEventId="1073741825"
segmentationEventCancelIndicator="false" segmentationDuration="450000">
        <scte35:DeliveryRestrictions webDeliveryAllowedFlag="false"
noRegionalBlackoutFlag="true" archiveAllowedFlag="true" deviceRestrictions="3"/>
      </scte35:SegmentationDescriptor>
    </scte35:SpliceInfoSection>
  </Event>
</EventStream>

```

```

    <scte35:SegmentationUpid segmentationUpidType="1" segmentationUpidLength="3"
    segmentationTypeId="48" segmentNum="0" segmentsExpected="0">012345</
scte35:SegmentationUpid>
    </scte35:SegmentationDescriptor>
  </scte35:SpliceInfoSection>
</Event>
</EventStream>

```

また、MediaPackage は、scte35:SpliceInsert メッセージをメタデータとして個々の動画セグメントに組み込みます。

ダウンストリーム広告サービスを使用している場合、そのサービスは MediaPackage が提供する マニフェスト内で SCTE-35 マーカーを検索し、それらのマーカーに基づいて広告を挿入します。

## 圧縮された DASH マニフェスト

DASH マニフェストを圧縮して低電力デバイスでの VOD とライブの両方のパフォーマンスと処理を向上させる機能を AWS Elemental MediaPackage で利用できます。

MediaPackage で提供されるデフォルトの DASH マニフェストには、各表現 (トラック) に関する重複データが含まれています。一部のプレーヤーでは、このすべてのデータを含むマニフェストの処理は困難で時間がかかります。MediaPackage では、この負荷の一部を減らすため、Representation オブジェクトから AdaptationSet オブジェクトに一部の属性を移動することで、マニフェストを圧縮できます。この方法では、マニフェストで各表現に対して属性を定義するのではなく、高いレベルで 1 回のみ定義します。これにより、表現が適応セットからこれらの属性を継承します。

### Example デフォルトの DASH マニフェスト

次の例では、SegmentTemplate オブジェクトとそのすべての要素が各 Representation. にリストされています。マニフェストの適用セットごとに、この同じレイアウトがあります。

```

<AdaptationSet mimeType="video/mp4" segmentAlignment="true" subsegmentAlignment="true"
startWithSAP="1" subsegmentStartsWithSAP="1" bitstreamSwitching="true">
  <Representation id="1" width="640" height="360" frameRate="30/1" bandwidth="749952"
codecs="avc1.640029">
    <SegmentTemplate timescale="30000" media="index_video_1_0_$.mp4?
m=1543947824" initialization="index_video_1_0_init.mp4?m=1543947824" startNumber="1">
      <SegmentTimeline>
        <S t="62000" d="60000" r="9"/>
      </SegmentTimeline>
    </Representation>
  </AdaptationSet>

```

```

    </SegmentTemplate>
  </Representation>
  <Representation id="2" width="854" height="480" frameRate="30/1" bandwidth="1000000"
  codecs="avc1.640029">
    <SegmentTemplate timescale="30000" media="index_video_3_0_${Number$.mp4?
m=1543947824" initialization="index_video_3_0_init.mp4?m=1543947824" startNumber="1">
      <SegmentTimeline>
        <S t="62000" d="60000" r="9"/>
      </SegmentTimeline>
    </SegmentTemplate>
  </Representation>
  <Representation id="3" width="1280" height="720" frameRate="30/1"
bandwidth="2499968" codecs="avc1.640029">
    <SegmentTemplate timescale="30000" media="index_video_5_0_${Number$.mp4?
m=1543947824" initialization="index_video_5_0_init.mp4?m=1543947824" startNumber="1">
      <SegmentTimeline>
        <S t="62000" d="60000" r="9"/>
      </SegmentTimeline>
    </SegmentTemplate>
  </Representation>
</AdaptationSet>

```

### Example 圧縮された DASH マニフェスト

この例では、SegmentTemplate オブジェクトとそのすべての要素が 1 つに折りたたまれ、AdaptationSet に移動されます。この再生デバイスは、この適応セットの各表現で、この同じテンプレートが使用されることを理解します。

```

<AdaptationSet mimeType="video/mp4" segmentAlignment="true" subsegmentAlignment="true"
startWithSAP="1" subsegmentStartsWithSAP="1" bitstreamSwitching="true">
  <SegmentTemplate timescale="30000" media="index_video_${RepresentationID$_
${Number$.mp4?m=1543947824" initialization="index_video_${RepresentationID$_
init.mp4?m=1543947824" startNumber="1">
    <SegmentTimeline>
      <S t="62000" d="60000" r="9"/>
    </SegmentTimeline>
  </SegmentTemplate>
  <Representation id="1" width="640" height="360" frameRate="30/1" bandwidth="749952"
codecs="avc1.640029"/>
  <Representation id="2" width="854" height="480" frameRate="30/1" bandwidth="1000000"
codecs="avc1.640029"/>
  <Representation id="3" width="1280" height="720" frameRate="30/1"
bandwidth="2499968" codecs="avc1.640029"/>

```

```
</AdaptationSet>
```

DASH マニフェストの圧縮の詳細については、「[AWS Elemental MediaPackage がマニフェストを圧縮する方法](#)」を参照してください。

## AWS Elemental MediaPackage でマニフェストを圧縮する方法

AWS Elemental MediaPackage コンソールから DASH マニフェストを圧縮するには、DASH エンドポイントの [マニフェストのレイアウト] で、[コンパクト] を選択します。適切なタイミングで利用可能なトラックを用意するために、MediaPackage はソースコンテンツのフレームレートとオーディオサンプリングレートを確認し、マニフェストが圧縮可能であるかどうか判断します。

### Note

キャプショントラックでは常に同じレートが使用されるため、MediaPackage は必ずキャプションを含めて適応セットを圧縮します。

MediaPackage は以下のアクションを実行します。

- このレートが適応セットのすべての表現で同じである場合、MediaPackage はすべての SegmentTemplate オブジェクトを 1 つに折りたたみ、これを AdaptationSet レベルに移動します。これにより、テンプレート内の情報がマニフェスト全体で繰り返されることはなくなります。表現間での同じテンプレートの使用を再生デバイスに許可するため、MediaPackage は、media および initialization リクエストの URL に \$RepresentationID\$ 変数を追加します。再生デバイスでは、この変数を、現在リクエスト中の表現の ID に置き換えます。ContentProtection 要素が存在する場合、MediaPackage はその要素も適応セットに移動します。
- 表現間でレートが異なる場合、MediaPackage は、最も頻繁に使用されているレートで SegmentTemplate を圧縮し、AdaptationSet に移動します。レートが異なる表現では、セグメントテンプレートが維持されます。表現のレートは、適応セットのレートを上書きします。
- 動画適応セットで明確に 2 つのフレームレートが使用されている場合、MediaPackage は以下のように圧縮します。
  - 24 と 48 が使用されている場合、圧縮されたテンプレートではフレームレートに 48 が使用され、タイムベースに 48000 が使用されます。
  - 25 と 50 が使用されている場合、圧縮されたテンプレートではフレームレートに 50 が使用され、タイムベースに 50000 が使用されます。



- 29.97 と 59.94 が使用されている場合、圧縮されたテンプレートではフレームレートに 59.95 が使用され、タイムベースに 60000 が使用されます。
- 30 と 60 が使用されている場合、圧縮されたテンプレートではフレームレートに 60 が使用され、タイムベースに 60000 が使用されます。

2つのビデオフレームレートが使用されているが、上記の倍増パターンのいずれかではない場合、そのセットを圧縮することはできません。

- 適応セットの表現間に重複したレートがない場合、そのセットを圧縮することはできません。

## DASH マニフェストのセグメントテンプレート形式

DASH セグメントテンプレートの形式を選択する機能は、AWS Elemental MediaPackage のライブワークフローでのみ使用できます。

以下のセクションでは、マニフェスト DASH で SegmentTemplate オブジェクトを変更して、再生デバイスの要件により適切に合わせる方法について説明します。

### トピック

- [SegmentTemplate での media 属性](#)
- [SegmentTemplate での duration 属性](#)

## SegmentTemplate での media 属性

SegmentTemplate プロパティの media 属性は、再生デバイスがセグメントリクエストを送信する URL を定義します。デフォルトでは、この URL は \$Number\$ 変数を使用して、リクエストされた特定のセグメントを識別します。再生デバイスがセグメントをリクエストすると、変数が、セグメントの数値 ID に置き換えられます。表現の最初のセグメントでは、この ID を、SegmentTemplate プロパティの startNumber の値と置き換えます。追加のセグメントごとに 1 ずつ増加します。

一部のプレーヤーでは、再生可能になると、タイムスタンプではなくセグメントが識別されたときに、セグメントのナビゲーションが向上します。このユースケースをサポートするために、MediaPackage は media 属性の URL に対し、\$Number\$ ではなく \$Time\$ 変数を使用します。再生デバイスがセグメントをリクエストすると、変数が、セグメントの可能な開始時刻に置き換えられます。この開始時刻は、SegmentTimeline オブジェクトのセグメント (S) プロパティの t 値で識別されます。例については、「[仕組み](#)」を参照してください。

## \$Time\$ 変数の動作について

「[DASH エンドポイントの作成](#)」で説明されているように、DASH エンドポイントでの [セグメントテンプレートフォーマット] 設定により \$Time\$ 変数を有効にします。AWS Elemental MediaPackage は次の処理を行います。

1. 次の例に示すように、MediaPackage が DASH マニフェストを生成する際、SegmentTemplate オブジェクトの media 値で変数 \$Time\$ が使用されます。

### Example

```
<SegmentTemplate timescale="30" media="index_video_1_0_-$Time$.mp4?m=1122792372"
  initialization="index_video_1_0_init.mp4?m=1122792372" startNumber="2937928">
```

2. 再生デバイスがセグメントをリクエストすると、media 属性で定義されている URL を使用して、リクエストされたセグメントの可能な開始時刻で、変数が置き換えられます。

### ⚠ Important

変数を置き換える値は、セグメントの正確な t 値である必要があります。リクエストで、任意のタイムスタンプを使用する場合、MediaPackage は最も近いセグメントをシークしません。

### Example

表現のセグメントテンプレートの例を次に示します。この例では \$Time\$ 変数を使用しています。

```
<SegmentTemplate timescale="30000" media="155_video_1_2_-$Time$.mp4?m=1545421124"
  initialization="155_video_1_2_init.mp4?m=1545421124" startNumber="710">
  <SegmentTimeline>
    <S t="255197799" d="360360" r="8"/>
    <S t="258441039" d="334334"/>
  </SegmentTimeline>
</SegmentTemplate>
```

最初のセグメントのリクエスト URL は **155\_video\_1\_2\_255197799.mp4** です。継続期間 360360 により、次のセグメントリクエストは **155\_video\_1\_2\_25558159.mp4** になり、以降同様に 9 番目のセグメントまで続きます。

最後のセグメントリクエストは **155\_video\_1\_2\_258441039.mp4** です。

## SegmentTemplate での duration 属性

デフォルトの DASH マニフェストでは、SegmentTemplate が SegmentTimeline を保持します。タイムラインは、その有効期間とその開始時刻を含め、Representation 内のすべてのセグメントについて説明しています。AWS Elemental MediaPackage では、ライブイベントにより、エンコーダーから受信すると、セグメントをタイムラインに追加します。新しく利用可能なセグメントを認識するために、再生デバイスは、更新されたマニフェストを定期的に MediaPackage に対しリクエストする必要があります。

ある表現内のすべてのセグメントの再生時間が同じである場合、MediaPackage を有効にして SegmentTimeline オブジェクトを削除することで、レイテンシーを軽減し、マニフェストを短縮できます。その代わりに、MediaPackage により SegmentTemplate プロパティに duration 属性が追加されます。再生デバイスは、duration と startNumber を使用して、セグメントがいつ利用できるかを計算します。再生デバイスは、セグメントについて知るために更新されたマニフェストに依存する必要がないため、再生を維持するために常に更新をリクエストする必要がありません。duration 属性の動作方法については、以下のセクションを参照してください。

### トピック

- [duration 属性の動作について](#)
- [duration 属性と圧縮された DASH マニフェスト](#)

### duration 属性の動作について

「[DASH エンドポイントの作成](#)」で説明されているように、DASH エンドポイントでの [セグメント テンプレートフォーマット] 設定により \$duration\$ 属性を有効にします。マニフェストでは次のような処理が実行されます。

1. AWS Elemental MediaPackage が DASH マニフェストを生成するとき、次の例に示すように、duration 属性が SegmentTemplate オブジェクトに追加されます。

#### Example

```
<SegmentTemplate timescale="30000" media="index_video_1_0_${Number$.mp4?m=1535562908" initialization="index_video_1_0_init.mp4?m=1535562908" startNumber="175032" duration="90000" presentationTimeOffset="62061"/>
```

セグメントタイムラインと個々のセグメントの説明は、セグメントテンプレートに含まれません。

### ⚠ Important

最終セグメントを除き、セグメントの所要時間の値からの逸脱は 50% 以下にする必要があります。期間が 90000 の場合、セグメントは 45000 ~ 135000 (30000 のタイムスケールにおいて 1.5 ~ 4.5 秒) の間である必要があります。

## Example

次に、セグメントテンプレートで `duration` を使用する適応セットの例を示します。

```
<AdaptationSet mimeType="video/mp4" segmentAlignment="true"
  subsegmentAlignment="true" startWithSAP="1" subsegmentStartsWithSAP="1"
  bitstreamSwitching="true">
  <Representation id="1" width="852" height="480" frameRate="30/1"
    bandwidth="1200000" codecs="avc1.4D401F">
    <SegmentTemplate timescale="30000" media="index_video_1_0_$.Number
$.mp4?m=1535562908" initialization="index_video_1_0_init.mp4?m=1535562908"
startNumber="175032" duration="90000" presentationTimeOffset="62061"/>
  </Representation>
  <Representation id="2" width="640" height="360" frameRate="30/1" bandwidth="800000"
    codecs="avc1.4D401E">
    <SegmentTemplate timescale="30000" media="index_video_3_0_$.Number
$.mp4?m=1535562908" initialization="index_video_3_0_init.mp4?m=1535562908"
startNumber="175032" duration="90000" presentationTimeOffset="62061"/>
  </Representation>
  <Representation id="3" width="320" height="240" frameRate="30/1" bandwidth="499968"
    codecs="avc1.4D400D">
    <SegmentTemplate timescale="30000" media="index_video_5_0_$.Number
$.mp4?m=1535562908" initialization="index_video_5_0_init.mp4?m=1535562908"
startNumber="175032" duration="90000" presentationTimeOffset="62061"/>
  </Representation>
</AdaptationSet>
```

- 再生デバイスは、`media` 属性で定義されている URL を使用してセグメントをリクエストします。URL では、最初のセグメントの `SegmentTemplate` にある `startNumber` の値から始めて、`$.Number$` 変数をセグメントの数に置き換えます。

3. 再生デバイスが最新のセグメントを決定する必要がある場合は、次の式を使用します。

$$((\text{ウォールクロック時刻} - \text{availabilityStartTime}) / (\text{duration} / \text{timescale})) + \text{startNumber}$$

#### Example

再生デバイスは、以下の値で最新のセグメントを計算します。

- 再生デバイスのウォールクロック時間: 2018-11-16T19:18:30Z
- availabilityStartTime - マニフェストの MPD オブジェクトからの属性: 2018-11-16T19:08:30Z
- duration - マニフェストの SegmentTemplate オブジェクトからの属性: 90000
- timescale - SegmentTemplate からの属性: 30000
- startNumber - SegmentTemplate からの属性: 175032

使用する計算は  $((2018-11-16T19:18:30Z - 2018-11-16T19:08:30Z) / (90000/30000)) + 175032$

この計算が、(経過時間 600 秒) / (セグメント再生時間 3 秒) = 200 経過セグメント、になります。これらのセグメントを 175232 開始セグメントに追加すると、最新セグメントが 175032 になります。

#### duration 属性の制約事項

適切に再生し、競合する属性のセグメント再生時間の問題を回避するために、AWS Elemental MediaPackage では、duration 属性に以下の制限が適用されます。

- この機能は、エンドポイントを作成する場合のみ有効にすることができます。

DASH マニフェストに後で duration 属性を追加するためにエンドポイントを変更することはできません。これには、あるセグメントテンプレート形式から duration を使用する別の形式に変更することが関係しています。たとえば、SegmentTimeline で \$Time\$ 変数を使用し、次に duration で \$Number\$ 変数を編集するエンドポイントを作成することはできません。

- エンドポイントの作成時に設定した [セグメントの再生時間] 値を保持する必要があります。

セグメントの再生時間を変更するためにエンドポイントを編集することはできません。

- duration を使用するエンドポイントから単一期間の DASH マニフェストを生成する必要があります。

`duration` 属性で複数期間の DASH を使用することはできません。

- 取り込まれるストリームでは、標準のセグメンテーションケイデンスを使用する必要があります。
- 取り込まれるストリームで可変セグメント長を使用することはできません。SCTE-35 関連のセグメンテーションの場合がその例です。

## `duration` 属性と圧縮された DASH マニフェスト

圧縮されたマニフェストを `duration` 属性と組み合わせると、マニフェストのサイズをさらに減少できますが、大幅な減少ではありません。圧縮されたマニフェストには、適応セットごとに 1 つの `SegmentTimeline` と `SegmentTemplate` があります。`duration` 属性を使用する場合、AWS Elemental MediaPackage はセグメントタイムラインを削除します。両方の処理により、マニフェストには、適応セットごとに 1 つの `SegmentTemplate` があり、`SegmentTimeline` はありません。次の例を参照してください。

圧縮されたマニフェストの詳細については、「[圧縮された DASH マニフェスト](#)」を参照してください。

### Important

表現内のセグメントに意図的にサイズが異なるセグメントがある場合、`duration` 属性を使用しないでください。この処理は、セグメントが一貫したサイズである場合のみ有効です。

## Example

圧縮されたマニフェストの例を次に示します。

```
<AdaptationSet mimeType="video/mp4" segmentAlignment="true"
  subsegmentAlignment="true" startWithSAP="1" subsegmentStartsWithSAP="1"
  bitstreamSwitching="true">
  <SegmentTemplate timescale="30000" media="index_video_{$RepresentationID
  $_$_Number$.mp4?m=1543947824" initialization="index_video_{$RepresentationID
  $_$_init.mp4?m=1543947824" startNumber="1">
    <SegmentTimeline>
      <S t="62000" d="60000" r="9"/>
    </SegmentTimeline>
  </SegmentTemplate>
  <Representation id="1" width="640" height="360" frameRate="30/1"
  bandwidth="749952" codecs="avc1.640029"/>
```

```

    <Representation id="2" width="854" height="480" frameRate="30/1"
    bandwidth="1000000" codecs="avc1.640029"/>
    <Representation id="3" width="1280" height="720" frameRate="30/1"
    bandwidth="2499968" codecs="avc1.640029"/>
  </AdaptationSet>

```

duration の属性を含む圧縮されたマニフェストの例を次に示します。

```

<AdaptationSet mimeType="video/mp4" segmentAlignment="true"
  subsegmentAlignment="true" startWithSAP="1" subsegmentStartsWithSAP="1"
  bitstreamSwitching="true">
  <SegmentTemplate timescale="30000" media="index_video_${RepresentationID}
  $__${Number$.mp4?m=1543947824" initialization="index_video_${RepresentationID}
  $__init.mp4?m=1543947824" startNumber="1" duration="60000"/>

```

## マニフェストでのフィルタリング

マニフェストフィルタリングを使用すると、AWS Elemental MediaPackage により、再生リクエストに追加されたクエリで指定したパラメータに基づいて、クライアントマニフェストが動的に生成されます。これにより、プレミアム 4K HEVC コンテンツへの視聴者によるアクセスを制限したり、特定のデバイスタイプや音声サンプルレートの範囲をターゲットにしたりなどを、すべて単一のエンドポイントから行うことができます。以前は、この動作を実現するには複数のエンドポイントを設定する必要があります。MediaPackage 現在では、同じエンドポイントで異なるクライアントマニフェストを動的に生成するための費用対効果の高い方法が提供されます。

## マニフェストフィルタの使用

マニフェストフィルタを使用すると、結果として生じるマニフェストには、クエリで指定した特性に一致するオーディオストリームとビデオストリームのみが含まれます。マニフェストフィルタを使用しない場合、取り込まれたストリームはすべてエンドポイント出力ストリームに存在します。例外は、最小ビデオビットレートなど、エンドポイントにストリームフィルタを設定した場合です。そ



の場合、マニフェストフィルタはストリームフィルタの後に適用され、出力を歪める可能性があるため、推奨されません。

マニフェストフィルタリングは、でサポートされているすべてのエンドポイントタイプで使用できません MediaPackage。

- Apple HLS
- DASH-ISO
- Microsoft Smooth Streaming
- CMAF

マニフェストフィルタリングを使用するには、再生リクエストにaws.manifestfilterクエリパラメータを に追加してクエリ MediaPackage MediaPackage を評価し、それらのクエリパラメータに基づいてクライアントマニフェストを提供します。マニフェストクエリでは、大文字と小文字は区別されず、最大 1024 文字まで指定できます。クエリの形式が正しくない場合、またはクエリパラメータと一致するストリームがない場合、MediaPackage は不完全または空のマニフェストを返します。クエリ構文については、次のセクションを参照してください。

#### Note

Apple HLS または CMAF エンドポイントを使用している場合は、特別な条件が適用されます。これらの条件の詳細については、[HLS および CMAF マニフェストの特別な条件](#) を参照してください。

## クエリ構文

基本となるクエリパラメータは aws.manifestfilter で、その後にオプションのパラメータ名と値のペアが続きます。クエリを構築するには、MediaPackage エンドポイント URL の末尾?aws.manifestfilter=に を追加し、その後にパラメータ名と値が続きます。すべての使用可能なパラメータのリストについては、「[マニフェストフィルタクエリパラメータ](#)」を参照してください。

Apple HLS フィルタクエリは次のようになります。

```
https://example-mediapackage-endpoint.mediapackage.us-west-2.amazonaws.com/out/v1/examplemediapackage/index.m3u8?  
aws.manifestfilter=audio_sample_rate:0-44100;video_bitrate:0-2147483647;video_codec:US,de
```

次の表に、クエリ構文が表示されます。

クエリ文字列のコンポーネント	説明
?	クエリの先頭を示す制限された文字。
aws.manifestfilter =	名前と値のペアで構成されたパラメータが続くベースクエリ。すべての使用可能なパラメータのリストについては、 <a href="#">「マニフェストフィルタクエリパラメータ」</a> を参照してください。
:	パラメータ名と値を関連付けるために使用されます。例えば、 <i>parameter_name :value</i> などです。
;	複数のパラメータを含むクエリのパラメータを区切ります。例えば、「 <i>parameter1_name:value ;parameter2_name:minimumValue-maxValue</i> 」と入力します。
,	値のリストを区切ります。例えば、「parameter_name: <i>value1,value2,value3</i> 」と入力します。リスト内のカンマ区切り値は、OR 関係を意味します。
-	パラメータの最小値 - 最大値の範囲を定義するために使用します。例えば、「audio_sample_rate:0-44100 」と入力します。範囲内で数値が使用される場合、その数値は範囲定義に含まれます。つまり、ストリームは最小値以上で、最大値以下である必要があります。範囲の場合、最小値と最大値は必須です。サポートされている範囲値は 0 - 2147483647 です。

#### Note

Amazon を CDN CloudFront として使用する場合は、追加の設定が必要になる場合があります。詳細については、「[すべてのエンドポイントのキャッシュ動作を設定する](#)」を参照してください。

## マニフェストフィルタクエリパラメータ

MediaPackage では、次のクエリパラメータがサポートされています。

カテゴリ	名前	説明	例
音声	audio_bitrate	<ul style="list-style-type: none"> <li>オーディオビットレート (ビット/秒)。</li> <li>許容値: 含まれる範囲を定義するダッシュで集計された 2 つの整数。サポートされている範囲値は 0 - 2147483647 です。</li> </ul>	stream.mpd?aws.manifestfilter=audio_bitrate:0-2147483647
音声	audio_channels	<ul style="list-style-type: none"> <li>オーディオチャンネルの数。</li> <li>許容値: 含まれる範囲を定義するダッシュで集計された 2 つの整数。サポートされている範囲値は 1 - 32767 です。</li> </ul>	stream.mpd?aws.manifestfilter=audio_channels:1-8
音声	audio_codec	<ul style="list-style-type: none"> <li>オーディオコーデックタイプ。</li> <li>許容値: AACL、AACH、AC-3、EC-3。AC-3 と EC-3 には - を含める必要がありません。  値では大文字と小文字が区別されません。</li> </ul>	stream.mpd?aws.manifestfilter=audio_codec:AACL,AC-3
音声	audio_language	<ul style="list-style-type: none"> <li>エンコーダーパススルーから派生したオーディオ言語または機能コード。</li> <li>許容値: 2 文字または 4 文字の <a href="#">ISO-639-1</a> 言語コードなどの任意文字列。エンコーダーで設定されている言語文字列と同じものを使用する必要があります。</li> </ul>	stream.mpd?aws.manifestfilter=audio_language:fr,en-US,de

カテゴリ	名前	説明	例
		値では大文字と小文字が区別されません。	
音声	audio_sample_rate	<ul style="list-style-type: none"> <li>オーディオサンプルレート (Hz)。</li> <li>許容値: 含まれる範囲を定義するダッシュで集計された2つの整数。サポートされている範囲値は 0 - 2147483647 です。</li> </ul>	stream.mpd?aws.manifestfilter=audio_sample_rate:0-44100
サブタイトル	subtitle_language	<ul style="list-style-type: none"> <li>エンコーダーパススルーから派生したサブタイトル言語または機能コード。</li> <li>許容値: 2文字または4文字の <a href="#">ISO-639-1</a> 言語コードなどの任意文字列。エンコーダーで設定されている言語文字列と同じものを使用する必要があります。</li> </ul> <p>値では大文字と小文字が区別されません。</p>	stream.mpd?aws.manifestfilter=subtitle_language:en-US, hi

カテゴリ	名前	説明	例
動画	trickplay_height	<ul style="list-style-type: none"> <li>トリックプレイのイメージの高さ (ピクセル単位)。これは、1フレームのみと画像ベースのトリックプレイの両方に該当します。</li> </ul> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p><b>Note</b></p> <p>このパラメータを1フレームのみのトリックプレイで使用する場合、trickplay_height と video_height は類似した値になります。値が同じでない場合は、1フレームのみのトラックがマニフェストから削除されることがあります。</p> </div> <ul style="list-style-type: none"> <li>trickplay_height フィルターは DASH on VOD をタイリングする前に適用されます。</li> <li>許容値: 含まれる範囲を定義するダッシュで集計された2つの整数。サポートされている範囲値は 1 - 2147483647 です。</li> </ul>	stream.mpd?aws.manifestfilter=trickplay_height:200-1200

カテゴリ	名前	説明	例
動画	trickplay_type	<ul style="list-style-type: none"><li>トリックプレイトラックのタイプ。Iフレームまたはイメージのトリックプレイトラックでフィルターするか、none の値を使用してすべてのトリックプレイトラック (Iフレームとイメージの両方) を除外できます。</li><li>許容値: iframe、image、none。</li></ul> 値では大文字と小文字が区別されません。	stream.mpd?aws.manifestfilter=trickplay_type:iframe

カテゴリ	名前	説明	例
動画	video_bitrate	<ul style="list-style-type: none"><li>動画ビットレート (ビット/秒)。  <div data-bbox="678 390 800 426"><b>Note</b></div><p>このパラメータを使用する場合は、video_bitrate フィルタパラメータのみを使用してビデオビットレートを設定することをお勧めします。MediaPackage コンソールまたは を使用して、ビデオの最小ビットレートと最大ビットレートも設定しないでくださいAWS CLI。video_bitrate フィルタは、エンドポイントで作成されたビデオビットレート設定に適用されます。パラメータを使用し、コンソールまたは AWS CLI でビットレートを設定すると、出力が歪む可能性があります。</p></li></ul>	



カテゴリ	名前	説明	例
動画	video_codec	<ul style="list-style-type: none"><li>• 動画のコーデックタイプ。</li><li>• 許容値: H264、H265。</li></ul> 値では大文字と小文字が区別されません。	stream.mpd?aws.manifestfilter=video_codec:h264
動画	video_dynamic_range	<ul style="list-style-type: none"><li>• 動画のダイナミックレンジ。</li><li>• 許容値: hdr10、hlg、sdr。</li></ul> 値では大文字と小文字が区別されません。	stream.mpd?aws.manifestfilter=video_dynamic_range:hdr10
動画	video_framerate	<ul style="list-style-type: none"><li>• NTSC 形式の動画のフレームレート範囲。</li><li>• 許容値: 含まれる範囲を定義するダッシュで集計された 2 つの浮動小数点数。各数値には、最大 3 つのオプションの小数値を指定できます。例えば、29.97、29.764 などです。サポートされている範囲値は 1 - 999.999 です。</li></ul>	stream.mpd?aws.manifestfilter=video_framerate:23.976-30

カテゴリ	名前	説明	例
動画	video_height	<ul style="list-style-type: none"> <li>ビデオの高さ (ピクセル単位)。</li> </ul> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p><b>Note</b></p> <p>このパラメータを1フレームのみのトリックプレイで使用する場合、trickplay_height と video_height は類似した値になります。値が同じでない場合は、1フレームのみのトラックがマニフェストから削除されることがあります。</p> </div> <ul style="list-style-type: none"> <li>許容値: 含まれる範囲を定義するダッシュで集計された2つの整数。サポートされている範囲値は 1 - 32767 です。</li> </ul>	stream.mp d?aws.manifestfilter=video_height:720-1080

## マニフェストフィルタリングの例

以下は、マニフェストフィルタリングの例です。

Example 1: AVC および 44.1k 音声サンプルレートをサポートするプレーヤーをターゲットにする

視聴者は、AVC および 44.1k 音声サンプルレートのみをサポートできるデバイスでコンテンツを再生しています。video\_codec および audio\_sample\_rate を設定して、これらの要件に合わないストリームを除外します。

```
?aws.manifestfilter=audio_sample_rate:0-44100;video_codec:h264
```

Example 2: 4k HEVC コンテンツを制限する

4K HEVC ストリームは 15 Mbps で、他のすべてのストリームは 9 Mbps 未満です。ストリームセットから 4K ストリームを除外するには、しきい値を 9,000,000 ビット/秒に設定して、より高いビットレートを除外します。

```
?aws.manifestfilter=video_bitrate:0-9000000
```

Example 3: 23.976 ~ 30 フレーム/秒のビデオを含める

特定のフレームレート範囲内のビデオのみを含めるには、`video_framerate` を使用します。このパラメータには、最大 3 つのオプションの 10 進値を含む浮動小数点数を指定できます。

```
?aws.manifestfilter=video_framerate:23.976-30
```

## HLS および CMAF マニフェストの特別な条件

HLS または CMAF マニフェストを使用している場合は、これらの特別な条件が適用されます。

- HLS マニフェストの場合、除外されたオーディオストリームと多重化されているビデオストリームを削除しないように、オーディオレンディショングループを使用することを強くお勧めします。レンディショングループの詳細については、「[AWS Elemental MediaPackage のレンディショングループのリファレンス](#)」を参照してください。
- HLS および CMAF マニフェストでは、音声サンプルレートは通知されないため、この設定の元のマニフェスト、またはフィルタリングされたマニフェストを視覚的に確認することは容易ではありません。音声サンプルレートを確認するには、エンコーダーレベルおよび出力レベルで音声サンプルレートを確認します。
- HLS および CMAF マニフェストでは、バリエーションの BANDWIDTH 属性は、音声トラックの帯域幅を、ビデオトラックと多重化されているか、ビデオトラックが参照するオーディオレンディショントラックであるかにかかわらず、ビデオトラックに関連付けます。したがって、元のマニフェストとフィルタリングされたマニフェストを視覚的に検査して、`video_bitrate` フィルターが機能していることを確認することはできません。フィルタを確認するには、エンコーダーレベルと出力レベルでビデオビットレートを確認します。
- HLS および CMAF マニフェストの場合、ビットレートのプレイリストまたはセグメントにリクエストパラメータが追加されると、HTTP 400 エラーが発生します。

## エラー状態

次の表に一般的なエラー状態を示します。

エラー状態	例	HTTP ステータスコード
リストパラメータが見つからず、限定されたリストの一部でもない	?aws.manifestfilter=audio_language:dahlia	200
字幕ストリームのみがストリームに存在している	?aws.manifestfilter=audio_sample_rate:0-1;video_bitrate=0-1	200
フィルタパラメータが重複している	?aws.manifestfilter=audio_sample_rate:0-48000;aws.manifestfilter=audio_sample_rate:0-48000	400
無効なパラメータ	?aws.manifestfilter=donut_type:rhododendron	400
無効な範囲パラメータ	?aws.manifestfilter=audio_sample_rate:300-0	400
無効な範囲値 (INT_MAX 以上)	?aws.manifestfilter=audio_sample_rate:0-2147483648	400
正しい形式でないクエリ文字列	?aws.manifestfilter=audio_sample_rate:is:0-44100	400
パラメータ文字列が 1024 文字を超えている	?aws.manifestfilter=audio_language:abcdefghijklmnop....	400

エラー状態	例	HTTP ステータスコード
HLS または CMAF ビットレートマニフェストのクエリパラメータ	<code>index_1.m3u8?aws.manifestfilter=video_codec:h264</code>	400
セグメントリクエストのクエリパラメータ	<code>..._1.[ts mp4 vtt.].?aws.manifestfilter=video_codec:h264</code>	400
繰り返しクエリパラメータ	<code>?aws.manifestfilter=audio_sample_rate:0-48000;aws.manifestfilter=video_bitrate:0-1</code>	400
フィルタを適用すると、空のマニフェストになる (コンテンツには、クエリ文字列で定義された条件を満たすストリームがない)。	<code>?aws.manifestfilter=audio_sample_rate:0-1;video_bitrate=0-1</code>	400

## メタデータのパススルー

AWS Elemental MediaPackage は、ID3 とキー長値 (KLV) メタデータを、チャンネルの入力からチャンネル出力のストリームに自動的にパススルーします。メタデータのパススルーを有効にするために、エンドポイントの設定を調整する必要はありません。

MediaPackage によるメタデータの処理方法の詳細については、以下のセクションを参照してください。

### トピック

- [ID3 メタデータに関する考慮事項](#)
- [KLV メタデータに関する考慮事項](#)

## ID3 メタデータに関する考慮事項

Timed ID3 メタデータは、同期されたメタデータをストリームに追加するための汎用のメカニズムです。このメタデータは、インタラクティブなアプリケーションからオーディエンスの測定まで、さまざまな目的で使用されます。

サポートされている MediaPackage エンドポイントのタイプ

MediaPackage では、次のエンドポイントタイプで、ID3 メタデータをパススルーすることができます。

- ライブおよび VOD HLS、DASH、および CMAF エンドポイント

メタデータキャリッジ

以下の説明で、ID3 がメタデータとしてどのように伝送されるかを示します。

- HLS – メタデータは基本ストリーム内で伝送されます。詳細については、Apple Timed Metadata for HTTP Live Streaming リファレンスの「[section 2.0](#)」を参照してください。
- CMAF および DASH – メタデータは、イベントメッセージボックスバージョン 1 で伝送されます。詳細については、「[Carriage of ID3 Timed Metadata in CMAF](#)」を参照してください。イベントメッセージボックスには、scheme\_id\_uri フィールド (<https://aomedia.org/emsg/ID3> に設定) と value フィールド (0 に設定) が含まれています。

メタデータシグナリング

DASH マニフェストには、ID3 メタデータを使用するトラックを含む AdaptationSets の要素 `<InbandEventStream schemeIdUri="https://aomedia.org/emsg/ID3" value="0"/>` が含まれます。

HLS マニフェストには、特定のメタデータシグナリングはありません。

MediaLive の 設定

AWS Elemental MediaLive の [MediaPackage 出カグループ](#)では、[ID3 メタデータをパススルーする](#)か、[スケジュールを使用して ID3 メタデータを挿入](#)することで、ID3 メタデータを生成できます。

## KLV メタデータに関する考慮事項

KLV は、ストリームに同期メタデータを組み込むためのデータエンコーディング標準規格です。KLV でのバイナリ値を使用する性質は、メタデータのボリュームが重要な場合に効果を発揮します。KLV は、産業ユースケースにおける航空監視からセンサーデータの送信、さらにライブスポーツのユースケースでのアスリートや物体のリアルタイムの追跡までをカバーする、さまざまなユースケースに使用できます。

サポートされている MediaPackage エンドポイントのタイプ

MediaPackage では、次のエンドポイントタイプで、KLV メタデータをパススルーできます。

- DASH でのライブエンドポイント

### メタデータキャリッジ

メタデータは、[MISB ST 1910.1](#) 仕様で説明されているように、イベントメッセージボックスバージョン 1 で伝送されます。同期 KLVトラックの場合、イベントメッセージボックスには `scheme_id_uri` フィールド (`urn:misb:KLV:bin:1910.1` に設定) と `value` フィールド (`KLVx:01FC` に設定) が含まれています。非同期 KLVトラックの場合、この値フィールドには `KLVx:01BD` がセットされます。いずれの場合も、`x` はストリーム内のトラックのインデックスを意味します。

### メタデータシグナリング

DASH マニフェストには、KLV メタデータを使用するトラックを含む `AdaptationSets` の要素 `<InbandEventStream schemeIdUri="urn:misb:KLV:bin:1910.1" value="KLVx:01FC"/>` または `<InbandEventStream schemeIdUri="urn:misb:KLV:bin:1910.1" value="KLVx:01BD"/>` が含まれ、これは伝送されるトラックの同期性によります。

### MediaLive の設定

MediaLive チャンネルからの KLV メタデータをパスすることができます。詳細については、「AWS Elemental MediaLive ユーザーガイド」の「[klv](#)」を参照してください。



# AWS Elemental MediaPackage のレンディシヨングループの ファレンス

レンディシヨングループは、HLS と CMAF の出力で使用します。レンディシヨングループは、すべてのサブタイトルやオーディオトラックを収集し、それらをストリームのすべてのビデオレンディシヨンで使用できるようにします。レンディシヨングループを有効にすると、MediaPackage ではすべてのオーディオバリエーション (複数の異なる言語やコーデックなど) がグループにまとめられ、ビデオレンディシヨンで使用できるようになります。MediaPackage では、サブタイトルは 1 つのレンディシヨングループに自動的にまとめられます。

オーディオとサブタイトルトラックは、CMAF 出力のそれら自身のレンディシヨングループに配置する必要があります。

レンディシヨングループの使用が適切であるケースについて以下のセクションで説明します。

## Note

DASH と Microsoft Smooth Streaming では、レンディシヨングループを使用しません。すべてのオーディオ、ビデオ、サブタイトル/キャプションのトラックはプレーヤーに提供され、どれを再生で使用するかはプレーヤーで決定されるためです。

## レンディシヨングループの使用が適切であるケース

レンディシヨングループは、HLS と CMAF の出力のみで使用します。レンディシヨングループの利点は、ストリームに複数の言語や複数のオーディオコーデックがある場合に最も発揮されます。レンディシヨングループは以下のユースケースで使用してください。

## Note

レンディシヨングループを含むライブ HLS ストリームから Live-to-VOD アセットを収集すると、それらのグループもアセットに渡されます。

### • CMAF 出力で音声やサブタイトルトラックがある場合

CMAF は 1 つのレンディシヨングループにすべてのオーディオトラックをまとめ、別のグループにすべてのサブタイトルをまとめる必要があります。オーディオやサブタイトルを、ビデオトラックと MUX (マルチプレクサ) として扱うことはできません。

- 1 つ以上のビデオトラックと複数のオーディオ言語またはコーデック

レンディショングループを有効にすると、MediaPackage では、ビデオトラック間で共有できるよう、すべてのオーディオレンディションがまとめられます。これにより、すべてのビデオトラック間ですべてのオーディオオプションを複製する必要がなくなります。

- 複数のオーディオ専用トラックと複数のサブタイトルトラック

複数のオーディオトラックと複数のサブタイトルトラックの両方がレンディショングループにある場合は、すべてのオーディオオプションを任意のサブタイトルトラックと組み合わせることができます。

- 1 つのオーディオ専用トラックと複数のサブタイトルトラック

MediaPackage では、オーディオトラックを任意のサブタイトルで使用できるよう、サブタイトルトラックが 1 つのレンディショングループに自動的にまとめられます。この場合、オーディオは 1 つのみで、サブタイトルは既にグループ化されているため、MediaPackage にレンディショングループを使用するよう指定する必要はありません。

## レンディショングループの使用が適切でないケース

以下のユースケースでは、レンディショングループを使用できないか、使用しないようにします。

- ストリーム内に複数のビデオトラックがあるが、オーディオで使用できる言語やコーデックが 1 つのみである場合。複数のオーディオトラックで同じオーディオが使用され、レンディショングループも使用されている場合、レンディショングループ内で同じオーディオトラックが重複します (ビデオごとに 1 つずつ)。

オーディオとビデオはストリーム内でミックスしたままにし、レンディショングループを使用しないでください。

- DASH または Microsoft Smooth Streaming 出力。これらのプロトコルは、レンディショングループをサポートしていません。代わりに、出力ストリームにすべてのトラックが含まれ、どれを再生するかはプレーヤー側またはマニフェスト側のルール (言語やビットレートの選択など) に基づいてプレーヤーによって決定されます。

プレーヤーで使用可能なトラックを制限するには、MediaPackage コンソールまたは MediaPackage API からストリームの選択オプションを使用します。

# AWS Elemental MediaPackage の SCTE-35 メッセージオプション

このセクションでは、ライブ HLS、DASH、CMAF 出力で SCTE-35 メッセージがどのように処理されるかを設定するために AWS Elemental MediaPackage (MediaPackage) で提供されているオプションを説明します。Live-to-VOD アセットの場合、MediaPackage では、ライブストリームから収集されたアセットに SCTE-35 メッセージが渡されます。これらのオプションは、Microsoft Smooth Streaming あるいはビデオオンデマンド (VOD) 出力には適用されません。

SCTE-35 メッセージは、ソースコンテンツ内のビデオに付随します。出力用にコンテンツがパッケージ化されている場合、これらのメッセージにより、MediaPackage で広告マーカートを挿入する必要がある場所を示されます。デフォルトでは、MediaPackage によりソースコンテンツの次のメッセージタイプにマーカートが挿入されます。

- `splice_insert`
- 次のセグメンテーションタイプがある `time_signal`:
  - プロバイダー広告
  - ディストリビューター広告
  - プロバイダー配置機会
  - ディストリビューター配置機会

また、`time_signal` は `segmentation_descriptor` に配信制限のフラグを含む必要があります。

これらのコマンドがある場合、MediaPackage により対応する広告マーカートが出力マニフェストに挿入されます。

- HLS および CMAF 出力では、MediaPackage により EXT-X-CUE-OUT タグおよび EXT-X-CUE-IN タグが挿入されます。
- DASH 出力では、複数期間のマニフェストが有効化されている場合、MediaPackage により複数期間を作成する EventStream タグが挿入されます。

次のセクションでは、MediaPackage での SCTE-35 メッセージの処理動作を変更する方法を説明します。

## MediaPackage での SCTE-35 の設定

MediaPackage で、ソースコンテンツからの SCTE-35 メッセージとやり取りする方法を変更することができます。エンドポイントで次のように設定します。詳細については、次を参照してください。

- MediaPackage コンソールについては、「[the section called “エンドポイントの作成”](#)」を参照してください。
- MediaPackage API については、AWS Elemental MediaPackage ライブ API リファレンスの「[Origin\\_endpoints](#)」を参照してください。

### Important

MediaPackage での SCTE-35 メッセージの処理方法を変更するには、SCTE-35 の標準規格を理解する必要があります。最新の標準規格は、[SCTE 規格カタログ](#)でご覧いただけます。また、SCTE-35 がソースコンテンツで実装される方法についても理解しておく必要があります。

### 広告マーカ

この設定は、HLS および CMAF エンドポイントで使用できます。

広告マーカでは、SCTE-35 メッセージを検出したときに行われる MediaPackage の動作を指定することができます。オプションは次の通りです。

- None (なし) — MediaPackage では、SCTE-35 メッセージが無視されます。出力マニフェストに広告マーカは含まれません。
- SCTE-35 enhanced (SCTE-35 拡張) — MediaPackage での SCTE-35 メッセージ用の出力マニフェストに広告マーカおよびブラックアウトタグが含まれます。これらは、Customize ad triggers (カスタム広告トリガー) および Ads on delivery restrictions (広告配信制限) の要件を満たします。
- Passthrough (パススルー) — MediaPackage では、ソースコンテンツからすべての SCTE-35 メッセージがコピーされ、それらが出力マニフェストに挿入されます。

### カスタム広告トリガー

この設定は、HLS、DASH、CMAF のエンドポイントで使用できます。

Customize ad triggers (カスタム広告トリガー) では、MediaPackage が出力マニフェストで広告として扱う SCTE-35 メッセージのタイプを識別できます。

この設定を変更しない場合、MediaPackage ではこれらのメッセージタイプは広告として扱われます。

- スプライス挿入
- プロバイダー広告
- ディストリビューター広告
- プロバイダー配置機会
- ディストリビューター配置機会

## 広告配信制限

この設定は、HLS、DASH、CMAF のエンドポイントで使用できます。

Ads on delivery restrictions (広告配信制限) では、メッセージの `segmentation_descriptor` の配信制限フラグに基づいて、SCTE-35 メッセージが広告になる条件を設定できます。MediaPackage により、配信制限の条件を満たしている適切なタイプのメッセージの位置に、該当する広告マーカースが挿入されます。

この設定を変更しない場合、MediaPackage により、制限されていると分類されるメッセージ (配信制限フラグがあります) が出カマニフェストの広告マーカースに変換されます。

### Note

スプライス挿入 SCTE-35 メッセージには `segmentation_descriptor` がありません。[Customize ad triggers (カスタム広告トリガー)] でスプライス挿入を選択した場合、すべてのスプライス挿入は出カマニフェストで広告マーカースとなります。

## 使用方法

Ad markers (広告マーカース)、Customize ad triggers (カスタム広告トリガー)、および Ads on delivery restrictions (広告配信制限) の設定は連携して作用し、ソースコンテンツからの SCTE-35 メッセージに対する MediaPackage の動作を決定します。

ソースコンテンツに SCTE-35 メッセージがある場合、MediaPackage では、Ad markers (広告マーカース) で選択した値に基づいて次のアクションが実行されます。

- None (なし) の場合、MediaPackage では SCTE-35 メッセージに対して何も行われません。出カマニフェストには広告マーカースが挿入されません。

- Passthrough (パススルー) の場合、MediaPackage によりソースコンテンツからすべての SCTE-35 メッセージがコピーされ、出カマニフェストに挿入されます。
- SCTE-35 enhanced (SCTE-35 強化) の場合、MediaPackage では設定した要件を満たすメッセージがあるかの確認が行われます。入カマニフェストでは、MediaPackage により適用できるメッセージに該当する広告マーカースが挿入されます。要件を確認するため、MediaPackage では次が実行されます。
  1. [Customize ad triggers (カスタム広告トリガー)] で指定したメッセージタイプと一致する SCTE-35 メッセージがあるかを確認する
  2. 適切なタイプのメッセージに対して、segmentation\_descriptor の配信制限フラグが [Ads on delivery restrictions (広告配信制限)] で設定した条件を満たしているかを確認する
  3. 配信制限条件を満たしている適切なメッセージに対して、このチャプターで上述するように、出カマニフェストに広告マーカースを挿入します。
  4. 日付範囲の場合、HLS および CMAF の出カマニフェストで広告やプログラムの移行イベントをシグナリングするため、MediaPackage によって EXT-X-DATERANGE タグが挿入されます。

## EXT-X-DATERANGE 広告マーカース

日付範囲の広告マーカースは、ライブ HLS および CMAF マニフェストの広告やプログラムの移行を知らせるために使用されます。エンドポイントで日付範囲の広告マーカースを有効にすると、MediaPackage により SCTE-35 の time\_signal または splice\_insert タグがあるマニフェストに EXT-X-DATERANGE タグが挿入されます。EXT-X-DATERANGE は、EXT-X-PROGRAM-DATE-TIME タグとの連携に使われます。

HLS 用の EXT-X-DATERANGE および EXT-X-PROGRAM-DATE-TIME タグについての詳細は、「[HTTP Live Streaming 2nd Edition Specification](#)」を参照してください。

### コンソール経由での日付範囲の有効化

エンドポイントの作成または編集時に日付範囲の広告マーカースを有効にするには、MediaPackage コンソールの [パッケージの設定] > [追加設定] > [広告マーカース] で [日付範囲] を選択します。

また、[日付範囲] を選択すると、0 より大きい [プログラムの日付/時間間隔 (秒)] の値を入力する必要があります。プログラムの日付および時間間隔は、広告マーカースの設定として同じ [Additional configuration] (その他の設定) ペインに設定されます。

## AWS CLI による日付範囲の有効化

エンドポイントで日付範囲の広告マーカを有効にするには、AWS CLI で次のコマンドを実行して、お客様自身の情報で *region* を置き換えます。

```
aws --endpoint=https://mediapackage.region.amazonaws.com mediapackage --region region
create-origin-endpoint --channel-id test_channel --id hlsmuxed
--hls-package "{\"ProgramDateTimeIntervalSeconds\":60,\"AdMarkers\":\":\"DATERANGE\"}"
```

### Important

0 より大きい ProgramDateTimeIntervalSeconds の値を設定する必要があります。

## MediaPackage API または AWS SDK 経由での日付範囲の有効化

MediaPackage ライブ API または AWS SDK 経由で HLS エンドポイントの日付範囲の広告マーカを有効にする方法については、次を参照してください。

- [MediaPackage ライブ API リファレンス](#)
- [AWS SDK](#)

## CTE-35 EXT-X-DATERANGE のシグナリングを示す HLS マニフェストの例

MediaPackage によって生成されたこの HLS マニフェストの例では、EXT-X-DATERANGE および EXT-X-PROGRAM-DATE-TIME タグを使用して、ライブストリーム内のイベントがシグナリングされます。

### Note

EXT-X-DATERANGE タグの属性 DURATION、PLANNED-DURATION、および END-DATE は、オプションです。これらの属性が SCTE-35 の入力に存在しない場合、または MediaPackage API を使用してエンドポイントを作成する際に設定されていない場合、生成されたマニフェストからは省略されます。

```
#EXTM3U
```



```
#EXT-X-VERSION:3
#EXT-X-TARGETDURATION:8
#EXT-X-MEDIA-SEQUENCE:11
#EXT-X-DATERANGE:ID="2415919105",START-DATE="2020-05-03T00:01:00.018Z",PLANNED-
DURATION=29.988,SCTE35-
OUT=0xFC303000000002CDE400FFF00506FE00526C14001A021843554549900000017FC00000292EA80A04ABCD00013
#EXT-X-DATERANGE:ID="2147483649",START-DATE="2020-05-03T00:00:30.030Z",PLANNED-
DURATION=90.006,SCTE35-
CMD=0xFC303000000002CDE400FFF00506FE00293D6C001A021843554549800000017FFF00007B9ABC0A04ABCD00011
#EXT-X-PROGRAM-DATE-TIME:2020-05-03T00:01:08.040Z
#EXTINF:7.560,
../././././index_1_11.ts?m=1588607409
#EXTINF:7.560,
../././././index_1_12.ts?m=1588607409
#EXTINF:6.846,
../././././index_1_13.ts?m=1588607409
#EXT-X-DATERANGE:ID="2415919105",START-DATE="2020-05-03T00:01:00.018Z",END-
DATE="2020-05-03T00:01:30.006Z",DURATION=29.988
#EXTINF:0.714,
../././././index_1_14.ts?m=1588607409
#EXTINF:7.560,
../././././index_1_15.ts?m=1588607409
#EXTINF:7.560,
../././././index_1_16.ts?m=1588607409
#EXTINF:7.560,
../././././index_1_17.ts?m=1588607409
#EXTINF:6.636,
../././././index_1_18.ts?m=1588607409
#EXT-X-DATERANGE:ID="2147483649",START-DATE="2020-05-03T00:00:30.030Z",END-
DATE="2020-05-03T00:02:00.036Z",DURATION=90.006,SCTE35-
CMD=0xFC304A00000002CDE400FFF00506FE00A4D8280034021843554549800000017FC000000000000A04ABCD00011
#EXT-X-DATERANGE:ID="2147483650",START-DATE="2020-05-03T00:02:00.036Z",PLANNED-
DURATION=90.006,SCTE35-
CMD=0xFC304A00000002CDE400FFF00506FE00A4D8280034021843554549800000017FC000000000000A04ABCD00011
#EXTINF:0.924,
../././././index_1_19.ts?m=1588607409
#EXTINF:7.560,
../././././index_1_20.ts?m=1588607409
#EXT-X-PROGRAM-DATE-TIME:2020-05-03T00:02:08.520Z
#EXTINF:7.560,
../././././index_1_21.ts?m=1588607409
#EXT-X-ENDLIST
```

# AWS Elemental MediaPackage のタイムシフト表示のリファレンス

タイムシフト表示は AWS Elemental MediaPackage でのライブワークフローで使用できます。

タイムシフト表示とは、視聴者が「現在」より前の時点でライブストリームの視聴を開始して、すでに進行中の番組を最初から視聴したり、すでに完了した番組を視聴したりできることを意味します。は、最大 336 時間 (14 日) 経過したコンテンツについてタイムシフト表示 MediaPackage をサポートします。エンドポイントで [startover window (スタートオーバーウィンドウ)] を定義することにより、このコンテンツの一部またはすべてのタイムシフト表示を有効にできます。再生リクエストに有効な開始パラメータと終了パラメータが含まれている場合、そのウィンドウ内でコンテンツを再生できます。エンドポイントで設定されたウィンドウ外のコンテンツをリクエストすると、HTTP エラー 404 が発生します。

または、ライブストリームのクリップを収集し、ビデオオンデマンド (VOD) アセットとして使用可能にすることもできます。VOD アセットの収集については、「[AWS Elemental MediaPackage を使用した live-to-VOD アセットの作成](#)」を参照してください。

以下の手順で「現在」とは、エンコーダーからのソースコンテンツのプログラム日時 (PDT) に基づく現時刻です。ソースコンテンツに PDT 情報が含まれていない場合、「現在」は最新のセグメントの MediaPackage 取り込み時刻を指します。

タイムシフト表示を有効にするには

1. MediaPackage エンドポイントオブジェクトのスタートオーバーウィンドウの値を入力して、タイムシフト表示を有効にします。これは、MediaPackage コンソールまたは MediaPackage API を使用して実行できます。

スタートオーバーウィンドウ内の開始パラメータと終了パラメータを持つリクエストがこのエンドポイントに送信されると、はリクエストされた期間にマニフェスト MediaPackage を生成します。開始パラメータまたは終了パラメータがスタートオーバーウィンドウ外にある場合、再生リクエストは失敗します。開始/終了パラメータが使用されていない場合は、標準のマニフェストを生成します。

## Note

エンドポイントで最初にスタートオーバーウィンドウを作成するときに、マニフェストが実際の時間より遅れていることに気づく場合があります。これは、がウィンドウの先頭からマニフェストを塗り MediaPackage つぶし、「現在」まで動作するためです。し

たがって、スタートオーバーウィンドウが 24 時間の場合、は 24 時間前からマニフェストを MediaPackage 埋め、「現在」まで作業します。

2. コンテンツのリクエストに、必要に応じて、開始/終了パラメータが含まれていることを確認します。MediaPackage は、最大 24 時間のコンテンツのリクエストを受け入れます。

パッケージ別のパラメータの表記規則については、「[開始/終了パラメータのルール](#)」を参照してください。

開始/終了パラメータは、マニフェストの時間範囲を決定します。以下は、リクエストの開始および終了パラメータに基づいて予期される動作です。

- URL に開始パラメータと終了パラメータの両方を指定すると、結果のマニフェストでは、指定した開始パラメータと終了パラメータに対応する固定の開始時間と終了時間が設定されます。

終了時間が将来の時間であれば、マニフェストのタグはライブマニフェストと一貫しています。それ以外の場合、終了時間が過去の時間であれば、マニフェストのタグはビデオオンデマンド (VOD) マニフェストと一貫しています。マニフェストの違いの詳細については、[ライブおよび VOD マニフェストのリファレンス](#) を参照してください。

- 開始パラメータを指定して終了パラメータを指定しないと、結果のマニフェストでは、指定した開始パラメータに対応する固定の開始時間が設定され、マニフェストの終了はライブコンテンツの進行に応じて先に伸びます。

#### Note

HLS 出力の場合、多くの再生デバイスでは「現在」の時刻に再生が開始されます。再生ウィンドウの実際の開始時間からコンテンツを表示するために、視聴者は再生進行状況バーで戻ることができます。

- どちらのパラメータも指定しないと、標準のマニフェストが生成され、終了時間は設定されずに「現在」から始まります。
- 終了パラメータを指定して開始パラメータを指定していない場合、マニフェストはパラメータが指定されていない場合と同じ方法で生成されます。マニフェストは「現在」から始まりますが、終了時刻がありません。

### ⚠ Important

タイムシフト表示を使用する場合は、視聴者ごとに固有の開始時間または終了時間を生成するのではなく、プレーヤーセッションの全体にわたる再生ウィンドウを使用することをお勧めします。これにより、CDNでのキャッシュが向上し、MediaPackageレベルでこれらのリクエストに関連するスロットリングが発生する可能性を回避できます。

## 開始/終了パラメータのルール

開始/終了パラメータをタイムシフトマネIFESTの開始/終了を示します。再生デバイスでは、マネIFESTのリクエストの末尾にパラメータを付加するか、リクエスト内にパラメータを含めることができます。

いずれの場合でも、日付と時刻を以下のいずれかの形式で表記する必要があります。

- 2017-08-18T21:18:54+00:00 などの ISO 8601 の日付。ここで、-08:00 はタイムゾーン UTC -08:00 です。
- POSIX (またはエポック) 時間 (1503091134 など)

以下のトピックでは、パッケージタイプ別の場所に関するルールについて説明します。

## DASH パラメータのルール

DASH コンテンツに対する URL リクエストの開始/終了パラメータでは、標準のパラメータ表記を使用できます。または、これらのパラメータをパスの要素として URL に含めることができます。

- クエリパラメータ表記 — 開始/終了パラメータがリクエスト URL の末尾に含まれます。

### Example

```
https://cf98fa7b2ee4450e.mediapackage.us-east-1.amazonaws.com/out/v1/997cbb27697d4863bb65488133bff26f/sports.mpd?start=1513717228&end=1513720828
```

- パスの要素 — 開始/終了パラメータがリクエスト URL のパスに含まれます。

## Example

```
https://cf98fa7b2ee4450e.mediapackage.us-east-1.amazonaws.com/out/  
v1/997cbb27697d4863bb65488133bff26f/start/2017-12-19T13:00:28-08:00/end/  
2017-12-19T14:00:28-08:00/sports.mpd
```

## HLS と CMAF のパラメータのルール

HLS コンテンツに対する URL リクエストの開始/終了パラメータでは、標準のパラメータ表記を使用できます。または、これらのパラメータをパスの要素として URL に含めることができます。HLS と CMAF のルールは同じです。ただし、CMAF のエンドポイントにパスの要素を挿入する場合、その要素は URL のマニフェスト ID の後に入れる必要がある点が異なります。

- クエリパラメータ表記 — 開始/終了パラメータがリクエスト URL の末尾に含まれます。

### Example HLS

```
https://cf98fa7b2ee4450e.mediapackage.us-east-1.amazonaws.com/out/  
v1/064134724fd74667ba294657a674ae72/  
comedy.m3u8?start=2017-12-19T13:00:28-08:00&end=2017-12-19T14:00:28-08:00
```

### Example CMAF

```
https://cf98fa7b2ee4450e.mediapackage.us-east-1.amazonaws.com/out/  
v1/064134724fd74667ba294657a674ae72/manifest_id/  
news.m3u8?start=2018-04-04T01:14:00-08:00&end=2018-04-04T02:15:00-08:00
```

- パスの要素 — 開始/終了パラメータがリクエスト URL のパスに含まれます。

### Example HLS

```
https://cf98fa7b2ee4450e.mediapackage.us-east-1.amazonaws.com/out/  
v1/064134724fd74667ba294657a674ae72/start/1513717228/end/1513720828/comedy.m3u8
```

## Example CMAF

```
https://cf98fa7b2ee4450e.mediapackage.us-east-1.amazonaws.com/out/  
v1/064134724fd74667ba294657a674ae72/manifest_id/start/1522807213/end/1522800013/  
news.m3u8
```

## Microsoft Smooth Streaming のパラメーター

Microsoft Smooth Streaming コンテンツに対する URL リクエストの開始/終了パラメータはパスの要素として URL に含めることができます。

- パスの要素 — 開始/終了パラメータがリクエスト URL のパスに含まれます。

### Example

```
https://cf98fa7b2ee4450e.mediapackage.us-east-1.amazonaws.com/out/  
v1/1f76b3b4f94c44a485c0e4e560afe50e/start/1513717228/end/1513720828/drama.ism/  
Manifest
```

## AWS Elemental MediaPackage でトリックプレイを使用する

トリックプレイ再生は、トリックモードとも呼ばれ、デジタルビデオプレーヤーでコンテンツを巻き戻したり、早送りしたり、検索するときに、視聴者に視覚的な手がかりを提供するものです。これは、ビデオプレーヤーを使用しているユーザーがコンテンツのタイムラインのどこにいるかを可視化するのに役立ちます。

AWS Elemental MediaPackage では、1フレームおよび画像ベースのトリックプレイがライブとビデオオンデマンド (VOD) のワークフローでサポートされています。1フレームトリックプレイ再生の場合、は HLS マルチバリエーションプレイリストの最初のレンディションから1フレームトラック MediaPackage を生成します。画像ベースのトリックプレイ再生の場合、はアップストリームエンコーダーで設定した画像メディアプレイリストを MediaPackage 渡します。で1フレームおよび画像ベースのトリックプレイ再生を使用する方法については MediaPackage、このトピックのセクションを参照してください。

MediaPackage では、次のトリックプレイ再生タイプがサポートされています。

ライブワークフローでサポートされるトリックプレイ再生のタイプ

ストリーミングプロトコル	Iフレームのみ	画像ベース
Apple HLS	✓	✓
CMAF Apple HLS	✓	✓
DASH	✓	✓

## VOD ワークフローでサポートされるトリックプレイ再生のタイプ

ストリーミングプロトコル	Iフレームのみ	画像ベース
Apple HLS	✓	✓
CMAF Apple HLS	✓	✓
DASH	✓	✓

## トピック

- [Iフレームのプレイリストを使用してトリックプレイ再生を有効にする](#)
- [イメージメディアプレイリストを使用してトリックプレイ再生を有効にする](#)

## Iフレームのプレイリストを使用してトリックプレイ再生を有効にする

MediaPackage は、既存の VOD アセットまたはライブストリームから I フレームプレイリストを作成することで、ライブおよびオンデマンドのトリックプレイ再生をサポートします。I フレームのプレイリストには、プレーヤーが画像のサムネイルに使用する I フレームのみのビデオセグメントが含まれています。I フレームのプレイリストについての詳細は、HTTP Live Streaming 2nd Edition specification (<https://datatracker.ietf.org/doc/html/rfc8216#section-4.3.3.6>) を参照してください。

### I フレームのプレイリストを使用してトリックプレイ再生を有効にするには

- MediaPackage コンソールで、エンドポイントまたはパッケージ設定を作成または編集するときに I フレームのみのストリームを含めるを選択します。は、マニフェストの最初のレンディションから I フレームのみのストリーム MediaPackage を生成します。サービスは EXT-I-FRAMES-ONLY タグを出カマニフェストに挿入し、I フレーム専用再生リストを生成した上で、



それをストリームに含めます。この再生リストでは、早送りや巻き戻しなどのプレイヤー機能を利用できます。

## イメージメディアプレイリストを使用してトリックプレイ再生を有効にする

画像ベースのトリックプレイ再生を使用するには、アップストリームエンコーダーで、JPEG 画像セグメントを含む HLS 画像メディアプレイリストを作成します。MediaPackage は、画像セグメントを自動的に出力に渡します。これらのセグメントは、ビデオプレーヤーでビジュアルキューに使用されるサムネイル画像と画像のメタデータです。これらのセグメントは、[Image Media Playlist 仕様のバージョン 0.4](#) に準拠している必要があります。サービスでは、この仕様の時間ベースの実装がサポートされています。

イメージメディアプレイリストを生成するようにアップストリームエンコーダーを設定する方法については、「[イメージメディアプレイリストを生成するようにアップストリームエンコーダーを設定する](#)」を参照してください。

### 入力ソースの要件

HLS のソースコンテンツは次の要件を満たしている必要があります。

- 動画プレイリストを参照する HLS の親プレイリストには、EXT-X-IMAGE-STREAM-INF タグを含める必要があります。
- 動画プレイリストには、次のタグを含める必要があります。
  - セグメントのリストの上にある EXT-X-IMAGES-ONLY タグ。
  - タイルサムネイルを使用している場合は、タイル情報を指定している各画像セグメントの上の EXT-X-TILES タグです。タイルサムネイルは、VOD ワークフローでのみ使用できます。

#### Note

プレイヤーに最も正確なイメージ期間 MediaPackage を提供するために、タグ EXT-INF と EXT-X-TILES タグには小数期間を使用することをお勧めします。

- 20 MB 未満の有効な JPEG の画像ファイルである画像セグメントを使用する必要があります。タイルサムネイルの場合、JPEG のグリッドに複数のサムネイルを使用して画像セグメントを並べたり、1 つのタイルが JPEG 全体を占有できます。

- ライブの場合、各 JPEG には画像セグメントを 1 つだけ含める必要があります。エンコーダーでは、同じタイムスタンプで画像セグメントとビデオセグメントを生成する必要があります。

AWS Media Services を使用して、Image Media Playlist 仕様のバージョン 0.4 に準拠した HLS のソースをアップストリームエンコーダーに生成できます。詳細については、以下の [イメージメディアプレイリストを生成するようにアップストリームエンコーダーを設定する](#) セクションを参照してください。

## 制限事項

で画像ベースのトリックプレイ再生を使用する場合は、次の制限事項に注意してください  
MediaPackage。

- MediaPackage では、パッケージング設定のイメージセグメントは結合されません。例えば、セグメントの再生時間が 2 秒の画像アセットを持つ VOD アセットを取り込み、セグメントの出力時間を 6 秒に指定した場合、ビデオセグメントとオーディオセグメントは 6 秒の長さに結合されますが、画像セグメントは 2 秒のままになります。
- HLS プレーヤーの要件に応じて、トリックプレイ再生の画像の表示に EXT-X-PROGRAM-DATE-TIME タグが必要になる場合があります。これは、ライブワークフローと VOD ワークフローに適用されます。

## DASH で画像ベースのトリックプレイ再生を使用する際の考慮事項

MediaPackage は、VOD ワークフローでは単一またはタイルサムネイル、ライブワークフローでは単一サムネイルをサポートしています。HLS コンテンツは、[Image Media Playlist 仕様のバージョン 0.4](#) に準拠している必要があります。個別の要件については、次のパラグラフを参照してください。が DASH パッケージング設定またはエンドポイントからコンテンツを MediaPackage 出力する場合、サービスは [DASH-IF 相互運用性ポイント](#) 仕様 v4.3、セクション 6.2.6 に基づいてサムネイルを出力します。

このセクションの前に挙げた一般的な要件に加えて、DASH でトリックプレイ再生を使用する際は、次の要件と制限事項に注意してください。

- MediaPackage は、VOD ワークフローの DASH タイルサムネイルのみをサポートします。
- 一般に、セグメントの配置に影響するため、このサービスで NUMBER\_WITH\_DURATION を使用するパッケージング設定に対して複数期間 DASH を利用することはできません。この制限はトリックプレイ再生にも適用されます。

- このサービスでは、ライブおよび VOD の画像セグメントのタイムフォーマットが次のように生成されます。
  - ライブの場合、画像セグメントのタイムフォーマットは、オーディオおよび動画セグメントのエンドポイントのものと同じです。このフォーマットは、エンドポイントのセグメントテンプレートフォーマットで設定されます。例えば、エンドポイントのセグメントテンプレートフォーマットが NUMBER\_WITH\_TIMELINE の場合、画像セグメントではタイムフォーマットに NUMBER\_WITH\_TIMELINE が使用されます。
  - VOD の場合、画像セグメントではパッケージング設定用に設定したタイムフォーマットに関係なく NUMBER\_WITH\_DURATION が使用されます。例えば、パッケージング設定に NUMBER\_WITH\_TIMELINE のセグメントテンプレートフォーマットを選択した場合、ビデオとオーディオのアダプテーションセットでは NUMBER\_WITH\_TIMELINE が使用されますが、画像のアダプテーションセットでは NUMBER\_WITH\_DURATION が使用されます。

## イメージメディアプレイリストを生成するようにアップストリームエンコーダーを設定する

HLS のソースは [Image Media Playlist 仕様のバージョン 0.4](#) に準拠している必要があります。次の AWS のメディアサービスを使用して、この仕様に準拠した HLS ストリームを作成できます。詳細については、次のドキュメントを参照してください。

- Elemental Live ユーザーガイドの「[イメージメディアプレイリスト仕様によるトリックプレイトラック](#)」
- AWS Elemental MediaLive ユーザーガイドの「[イメージメディアプレイリスト仕様によるトリックプレイトラック](#)」
- AWS Elemental MediaConvert API リファレンスの [HlsImageBasedTrickPlay](#)

# のセキュリティ AWS Elemental MediaPackage

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

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

- **クラウドのセキュリティ** — クラウドで AWS サービスを実行するインフラストラクチャを保護する責任 AWS は AWS にあります。AWS また、では、安全に使用できるサービスも提供しています。[AWS コンプライアンスプログラム](#)の一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。に適用されるコンプライアンスプログラムの詳細については AWS Elemental MediaPackage、「[コンプライアンスAWS プログラムによる対象範囲内のサービス](#)」を参照してください。
- **クラウドのセキュリティ** — お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、の使用時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 MediaPackage。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 MediaPackage を達成するために を設定する方法を示します。また、MediaPackage リソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

## トピック

- [でのデータ保護 AWS Elemental MediaPackage](#)
- [の Identity and Access Management AWS Elemental MediaPackage](#)
- [でのログ記録とモニタリング AWS Elemental MediaPackage](#)
- [のコンプライアンス検証 AWS Elemental MediaPackage](#)
- [の耐障害性 AWS Elemental MediaPackage](#)
- [のインフラストラクチャセキュリティ AWS Elemental MediaPackage](#)

## でのデータ保護 AWS Elemental MediaPackage

責任 AWS [共有モデル](#)、でのデータ保護に適用されます AWS Elemental MediaPackage。このモデルで説明されているように、AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービスのセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「[データプライバシーのよくある質問](#)」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記事「[AWS 責任共有モデルおよび GDPR](#)」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 は必須であり TLS 1.3 がお勧めです。
- 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。
- AWS 暗号化ソリューションと、内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-2 検証済みの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 \(FIPS\) 140-2](#)」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、コンソール、API、MediaPackage または SDK を使用して AWS CLI または他の AWS のサービス を操作する場合も同様です。AWS SDKs 名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

### トピック

- [を使用した DRM の実装 AWS Elemental MediaPackage](#)
- [AWS Elemental MediaPackageでの CDN 認証の実装](#)

## を使用した DRM の実装 AWS Elemental MediaPackage

暗号化を使用して、コンテンツを不正アクセスから保護します。MediaPackage は、デジタル著作権管理 (DRM) をサポートしています。DRM を使用すると、コンテンツを配信後に認可された閲覧者のみが閲覧することを確実にできます。

で DRM を使用する方法については、MediaPackage「」を参照してください[AWS Elemental MediaPackage でのコンテンツの暗号化と DRM](#)。

## AWS Elemental MediaPackageでの CDN 認証の実装

コンテンツ配信ネットワーク (CDN) 認証を使用して、許可されたデバイスだけがコンテンツにアクセスできるようにします。CDN 認証では、再生リクエストには、作成した適切なヘッダーと認証コードを含める必要があります。MediaPackage は、正しいコードを含まない再生リクエストを拒否します。

CDN 認証の詳細については、「[AWS Elemental MediaPackage での CDN 認証](#)」を参照してください。

## の Identity and Access Management AWS Elemental MediaPackage

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つです。IAM 管理者は、誰を認証 (サインイン) し、誰に MediaPackage リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

### トピック

- [対象者](#)
- [アイデンティティを使用した認証](#)
- [ポリシーを使用したアクセスの管理](#)
- [が IAM と AWS Elemental MediaPackage 連携する方法](#)
- [のアイデンティティベースのポリシーの例 MediaPackage](#)
- [AWS Secrets Managerのシークレットのための IAM ポリシー例](#)



- [サービス間での不分別な代理処理の防止](#)
- [MediaPackage ID とアクセスのトラブルシューティング](#)
- [詳細はこちら](#)
- [MediaPackage のサービスにリンクされたロールの使用](#)

## 対象者

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

サービスユーザー – MediaPackage サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの MediaPackage 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解しておく、管理者に適切な許可をリクエストするうえで役立ちます。の機能にアクセスできない場合は、MediaPackage 「」を参照してください [MediaPackage ID とアクセスのトラブルシューティング](#)。

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

IAM 管理者 - IAM 管理者は、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 MediaPackage。IAM で使用できる MediaPackage アイデンティティベースのポリシーの例を表示するには、「」を参照してください [アイデンティティベースのポリシーの例 MediaPackage](#)。

## アイデンティティを使用した認証

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

ID ソースを通じて提供された認証情報を使用して、フェデレーテッド ID AWS としてにサインインできます。AWS IAM Identity Center (IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーテッド ID の例です。フェデレーテッドアイデンティティとしてサインインする場合、IAM ロールを使用して、前もって管理者により ID



フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「ユーザーガイド」の「[へのサインイン AWS アカウント](#)方法AWS サインイン」を参照してください。

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、IAM [ユーザーガイドの API AWS リクエスト](#)の署名を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、AWS では、多要素認証 (MFA) を使用してアカウントのセキュリティを向上させることをお勧めします。詳細については、『AWS IAM Identity Center ユーザーガイド』の「[Multi-factor authentication](#)」(多要素認証) および『IAM ユーザーガイド』の「[AWSにおける多要素認証 \(MFA\) の使用](#)」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「[ルートユーザー認証情報が必要なタスク](#)」を参照してください。

## フェデレーテ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、一時的な認証情報を使用して にアクセスするための ID プロバイダーとのフェデレーションの使用を要求 AWS のサービス します。

フェデレーテッド 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のユーザー、または ID ソースを通じ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ことも、独自の ID ソース内のユーザーとグループのセットに接続して同期して、すべての AWS アカウント とアプリケーションで使用することもできます。IAM Identity Center の詳細については、『AWS IAM Identity Center ユーザーガイド』の「[What is IAM Identity Center?](#)」(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 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「[長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする](#)」を参照してください。

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

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

## IAM ロール

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

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス - フェデレーテッドアイデンティティに権限を割り当てるには、ロールを作成してそのロールの権限を定義します。フェデレーテッドアイデンティティが認証されると、そのアイデンティティはロールに関連付けられ、ロールで定義されている権限が付与されます。フェデレーションの詳細については、『IAM ユーザーガイド』の「[サードパーティーアイデンティティプロバイダー向けロールの作成](#)」を参照してください。IAM アイデンティティセンターを使用する場合、権限セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。権限セットの詳細については、『AWS IAM Identity Center ユーザーガイド』の「[権限セット](#)」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の AWS のサービス、(ロールをプロキシとして使用する代わりに) 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 ロールとリソースベースのポリシーとの相違点](#)」を参照してください。
- クロスサービスアクセス — 一部の 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権限、サービスロール、またはサービスにリンクされたロールを使用してこれを行う場合があります。
- 転送アクセスセッション (FAS) — IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「[転送アクセスセッション](#)」を参照してください。
- サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける [IAM ロール](#)です。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細に

については、「IAM ユーザーガイド」の「[AWS のサービスに権限を委任するロールの作成](#)」を参照してください。

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

IAM ロールと IAM ユーザーのどちらを使用するかについては、『IAM ユーザーガイド』の「[\(IAM ユーザーではなく\) IAM ロールをいつ作成したら良いのか?](#)」を参照してください。

## ポリシーを使用したアクセスの管理

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

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

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

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

## アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「[IAM ポリシーの作成](#)」を参照してください。

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

## リソースベースのポリシー

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

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

## アクセスコントロールリスト (ACL)

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



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

## その他のポリシータイプ

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

- **アクセス許可の境界** - アクセス許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。Principal フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。許可の境界の詳細については、「IAM ユーザーガイド」の「[IAM エンティティの許可の境界](#)」を参照してください。
- **サービスコントロールポリシー (SCPs)** - SCPs は、の組織または組織単位 (OU) に対する最大アクセス許可を指定する JSON ポリシーです AWS Organizations。AWS Organizations は、AWS アカウント ビジネスが所有する複数の をグループ化して一元管理するサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、『AWS Organizations ユーザーガイド』の「[SCP の仕組み](#)」を参照してください。
- **セッションポリシー** - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合があります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「[セッションポリシー](#)」を参照してください。

## 複数のポリシータイプ

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

## が IAM と AWS Elemental MediaPackage 連携する方法

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

で使用できる IAM の機能 MediaPackage

IAM 機能	MediaPackage サポート
<a href="#">アイデンティティベースのポリシー</a>	Yes
<a href="#">リソースベースのポリシー</a>	No
<a href="#">ポリシーアクション</a>	Yes
<a href="#">ポリシーリソース</a>	はい
<a href="#">ポリシー条件キー (サービス固有)</a>	はい
<a href="#">ACL</a>	No
<a href="#">ABAC (ポリシー内のタグ)</a>	はい
<a href="#">一時的な認証情報</a>	Yes
<a href="#">プリンシパル権限</a>	Yes
<a href="#">サービスロール</a>	あり
<a href="#">サービスリンクロール</a>	部分的

MediaPackage 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を把握するには、「IAM ユーザーガイド」の「IAM [AWS と連携する のサービス](#)」を参照してください。

### のアイデンティティベースのポリシー MediaPackage

アイデンティティベースポリシーをサポートする	Yes
------------------------	-----



アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、『IAM ユーザーガイド』の「[IAM ポリシーの作成](#)」を参照してください。

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は、「IAM ユーザーガイド」の「[IAM JSON ポリシーの要素のリファレンス](#)」を参照してください。

のアイデンティティベースのポリシーの例 MediaPackage

MediaPackage アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいの [アイデンティティベースのポリシーの例 MediaPackage](#)。

内のリソースベースのポリシー MediaPackage

リソースベースのポリシーのサポート	No
-------------------	----

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

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 がある場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリ

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追加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 ロールとリソースベースのポリシーとの相違点](#)」を参照してください。

## のポリシーアクション MediaPackage

ポリシーアクションに対するサポート	はい
-------------------	----

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

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権限のみのアクションなど、いくつかの例外があります。また、ポリシーに複数アクションが必要なオペレーションもあります。これらの追加アクションは、**依存アクション**と呼ばれます。

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

MediaPackage アクションのリストを確認するには、「サービス認証リファレンス」の「[で定義されるアクション AWS Elemental MediaPackage](#)」を参照してください。

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

```
mediapackage
```

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

ワイルドカード (\*) を使用して複数アクションを指定できます。例えば、Describe という単語で始まるすべてのアクションを指定するには、次のアクションを含めます。

```
"Action": "mediapackage:Describe*"
```

MediaPackage アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいの [アイデンティティベースのポリシーの例 MediaPackage](#)。

## のポリシーリソース MediaPackage

ポリシーリソースに対するサポート	はい
------------------	----

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

Resource JSON ポリシー要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource 要素を含める必要があります。ベストプラクティスとして、[Amazon リソースネーム \(ARN\)](#) を使用してリソースを指定します。これは、リソースレベルの権限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": "*"
```

MediaPackage には次のリソース ARNs。

```
arn:${Partition}:mediapackage:${Region}:${Account}:channels/${channelID}
arn:${Partition}:mediapackage:${Region}:${Account}:origin_endpoints/${endpointID}
```

ARN の形式の詳細については、「Amazon [リソースネーム \(ARNs AWS 「サービス名前空間」](#)」を参照してください。

たとえば、ステートメントで 9a6b3953e242400eb805f324d95788e3 チャンネルを指定するには、次の ARN を使用します。

```
"Resource": "arn:aws:mediapackage:us-east-1:111122223333:channels/9a6b3953e242400eb805f324d95788e3"
```

特定のアカウントに属するすべてのインスタンスを指定するには、ワイルドカード (\*) を使用します。

```
"Resource": "arn:aws:mediapackage:us-east-1:111122223333:channels/*"
```

リソースを作成するための MediaPackage アクションなど、一部のアクションは、特定のリソースで実行できません。このような場合は、ワイルドカード \* を使用する必要があります。

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

MediaPackage リソースタイプとその ARNs」の「[で定義されるリソース AWS Elemental MediaPackage](#)」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 Elemental MediaPackageで定義されるアクション](#)」を参照してください。

MediaPackage アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいの [アイデンティティベースのポリシーの例 MediaPackage](#)。

## のポリシー条件キー MediaPackage

サービス固有のポリシー条件キーのサポート	はい
----------------------	----

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

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

1 つのステートメントに複数の Condition 要素を指定するか、1 つの Condition 要素に複数のキーを指定すると、AWS は AND 論理演算子を使用してそれら进行评估します。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「[IAM ポリシーの要素: 変数およびタグ](#)」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 [AWS 「グローバル条件コンテキストキー」](#) を参照してください。

MediaPackage 条件キーのリストを確認するには、「サービス認証リファレンス」の「[条件キー AWS Elemental MediaPackage](#)」を参照してください。条件キーを使用できるアクションとリソースについては、「[定義されるアクション AWS Elemental MediaPackage](#)」を参照してください。

MediaPackage アイデンティティベースのポリシーの例を表示するには、「[」](#)を参照してくださいの [アイデンティティベースのポリシーの例 MediaPackage](#)。

## ACLs MediaPackage

ACL のサポート

No

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための権限を持つかを制御します。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。

## での ABAC MediaPackage

ABAC のサポート (ポリシー内のタグ)

はい

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アクセス許可戦略です。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操作を許可するように ABAC ポリシーを設計します。

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/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの [条件要素](#) でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値ははいです。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「[ABAC とは?](#)」を参照してください。ABAC をセットアップするステップ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「[属性に基づくアクセスコントロール \(ABAC\) を使用する](#)」を参照してください。

## での一時的な認証情報の使用 MediaPackage

一時的な認証情報のサポート	はい
---------------	----

一部の は、一時的な認証情報を使用してサインインすると機能 AWS のサービスしません。一時的な認証情報 AWS のサービス を使用する などの詳細については、IAM ユーザーガイドの[AWS のサービス「IAM 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、一時的な認証情報を使用します。例えば、会社の Single Sign-On (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「[ロールへの切り替え \(コンソール\)](#)」を参照してください。

一時的な認証情報は、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 にアクセスします AWS。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。

## のクロスサービスプリンシパル許可 MediaPackage

フォワードアクセスセッション (FAS) をサポート	はい
----------------------------	----

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 へのリクエストリクエストリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のア

クシオ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。

## MediaPackage のサービスロール

サービスロールに対するサポート	あり
-----------------	----

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 [IAM ロール](#) です。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「[AWS のサービスに権限を委任するロールの作成](#)」を参照してください。

### Warning

サービスロールのアクセス許可を変更すると、MediaPackage 機能が破損する可能性があります。が指示する場合以外 MediaPackage は、サービスロールを編集しないでください。

## での IAM ロールの選択 MediaPackage

でアセットリソースを作成するときは MediaPackage、 がユーザーに代わって Amazon S3 にアクセスすることを許可 MediaPackage するロールを選択する必要があります。以前にサービスロールまたはサービスにリンクされたロールを作成 MediaPackage したことがある場合は、 から選択できるロールのリストが提供されます。Amazon S3 バケットからの読み込みおよびコンテンツの取得へのアクセスを許可するロールを必ず選択してください。詳細については、「[他の AWS サービスへのアクセスを AWS Elemental MediaPackage に許可する](#)」を参照してください。

## のサービスにリンクされたロール MediaPackage

サービスリンクロールのサポート	部分的
-----------------	-----

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権限を表示できますが、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、「[IAM と提携するAWS のサービス](#)」を参照してください。表の中から、[Service-linked role] (サービスにリンクされたロール) 列に Yes と記載されたサービスを見つけます。サービス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] リンクを選択します。

## のアイデンティティベースのポリシーの例 MediaPackage

デフォルトでは、ユーザーとロールにはリソースを作成または変更 MediaPackage するアクセス許可はありません。また、AWS Command Line Interface ( AWS CLI ) AWS Management Console、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、リソースに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。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、『IAM ユーザーガイド』の「[IAM ポリシーの作成](#)」を参照してください。

各リソースタイプの ARN の形式など MediaPackage、で定義されるアクションとリソースタイプの詳細については、「サービス認証リファレンス」の「[のアクション、リソース、および条件キー](#) [AWS Elemental MediaPackage](#)」を参照してください。ARNs

### トピック

- [ポリシーのベストプラクティス](#)
- [MediaPackage コンソールを使用する](#)
- [自分の権限の表示をユーザーに許可する](#)

### ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが MediaPackage 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を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細につい

ては、『IAM ユーザーガイド』の「[AWS マネージドポリシー](#)」または「[AWS ジョブ機能の管理ポリシー](#)」を参照してください。

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

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

## MediaPackage コンソールを使用する

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

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

ユーザーとロールが MediaPackage 引き続きコンソールを使用できるようにするには、エンティティに MediaPackage *ReadOnly* AWS 管理ポリシーもアタッチします。詳細については、「IAM ユーザーガイド」の「[ユーザーへのアクセス許可の追加](#)」を参照してください。

## AWS Elemental MediaPackage ReadOnly

### 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:ListGroupsWithUser",
        "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 Secrets Managerのシークレットのための IAM ポリシー例

セットアップ時に、に割り当てる [IAM ポリシーを作成します](#) AWS Elemental MediaPackage。このポリシーにより、AWS Elemental MediaPackage は に保存したシークレットを読み取ることができます AWS Secrets Manager。このポリシーの設定はお客様の判断次第です。ポリシーは、最も制限の厳しい (特定のシークレットのみへのアクセスを許可する) から、最も制限の低い (この AWS アカウントを使用して作成するシークレットへのアクセスを許可する) までの範囲があります。ベストプラクティスとして、最も制限の厳しいポリシーを使用することをお勧めします。ただし、このセクションの例では、異なるレベルの制限を持つポリシーを設定する方法を説明します。AWS Elemental MediaPackage はシークレットへの読み取りアクセスのみを必要とするため、このセクションのすべての例には、保存した値を読み取るために必要なアクションのみが表示されます。

### トピック

- [で特定のシークレットへの読み取りアクセスを許可する AWS Secrets Manager](#)
- [の特定のリージョンで作成されたすべてのシークレットへの読み取りアクセスを許可する AWS Secrets Manager](#)
- [内のすべてのリソースへの読み取りアクセスを許可する AWS Secrets Manager](#)

### で特定のシークレットへの読み取りアクセスを許可する AWS Secrets Manager

次の IAM ポリシーは、で作成した特定のリソース (シークレット) への読み取りアクセスを許可します AWS Secrets Manager。

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "secretsmanager:GetResourcePolicy",  
        "secretsmanager:GetSecretValue",  
      ]  
    }  
  ]  
}
```

```

        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds"
    ],
    "Resource": [
        "arn:aws:secretsmanager:us-
west-2:111122223333:secret:aes128-1a2b3c",
        "arn:aws:secretsmanager:us-
west-2:111122223333:secret:aes192-4D5e6F",
        "arn:aws:secretsmanager:us-
west-2:111122223333:secret:aes256-7g8H9i"
    ]
    }
}

```

## の特定のリージョンで作成されたすべてのシークレットへの読み取りアクセスを許可する AWS Secrets Manager

次の IAM ポリシーは、の特定の AWS リージョンで作成したすべてのシークレットへの読み取りアクセスを許可します AWS Secrets Manager。このポリシーは、すでに作成したリソースと、指定したリージョンで将来作成するすべてのリソースに適用されます。

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetResourcePolicy",
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret",
                "secretsmanager:ListSecretVersionIds"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-west-2:111122223333:secret:*"
            ]
        }
    ]
}

```

## 内のすべてのリソースへの読み取りアクセスを許可する AWS Secrets Manager

次の IAM ポリシーは、AWS Secrets Manager で作成するすべてのリソースへの読み取りアクセスを許可します。このポリシーは、既に作成したリソースと、今後作成するすべてのリソースに適用されます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource": ["*"]
    }
  ]
}
```

## サービス間での不分別な代理処理の防止

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

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

混乱した代理問題から保護するための最も効果的な方法は、リソースの完全な ARN を指定して、`aws:SourceArn` グローバル条件コンテキストキーを使用することです。リソースの完全な ARN が不明な場合や、複数のリソースを指定する場合には、グローバルコンテキスト条件キー `aws:SourceArn` で、ARN の未知部分を示すためにワイルドカード文字 (\*) を使用します。例えば、`arn:aws:servicename:*:123456789012:*` です。

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

次の例は、`aws:SourceArn` および `aws:SourceAccount` のグローバル条件コンテキストキーを使用して MediaPackage、収集ジョブを使用する際の混乱した代理問題を防止する方法を示しています。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "mediapackage.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:mediapackage:*:123456789012:harvest_jobs/*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

## MediaPackage ID とアクセスのトラブルシューティング

次の情報は、IAM の使用時に発生する可能性がある一般的な問題の診断 MediaPackage と修正に役立ちます。

### トピック

- [でアクションを実行する権限がない MediaPackage](#)



- [iam を実行する権限がありません。PassRole](#)
- [自分の 以外のユーザーに自分の MediaPackage リソース AWS アカウント へのアクセスを許可したい](#)

## でアクションを実行する権限がない MediaPackage

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

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

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

この場合、mediapackage:*GetWidget* アクションを使用して *my-example-widget* リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

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

## iam を実行する権限がありません。PassRole

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して iam:PassRole を渡すことができるようにする必要があります MediaPackage。

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

次の例のエラーは、という IAM marymajor ユーザーがコンソールを使用して iam:PassRole アクションを実行しようする場合に発生します MediaPackage。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。Mary には、ロールをサービスに渡す権限がありません。

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

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

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

## 自分の 以外のユーザーに自分の MediaPackage リソース AWS アカウント へのアクセスを許可したい

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

詳細については、以下を参照してください:

- がこれらの機能 MediaPackage をサポートしているかどうかを確認するには、「」を参照してください [が IAM と AWS Elemental MediaPackage 連携する方法](#)。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、[IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」](#)を参照してください。
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、IAM ユーザーガイドの「[サードパーティー AWS アカウント が所有する へのアクセスを提供する](#)」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、『IAM ユーザーガイド』の「[外部で認証されたユーザー \(ID フェデレーション\) へのアクセス権限](#)」を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いの詳細については、『IAM ユーザーガイド』の「[IAM ロールとリソースベースのポリシーとの相違点](#)」を参照してください。

## 詳細はこちら

の ID とアクセスの管理の詳細については MediaPackage、次のページを参照してください。

- [が IAM と AWS Elemental MediaPackage 連携する方法](#)
- [のアイデンティティベースのポリシーの例 MediaPackage](#)

- [MediaPackage ID とアクセスのトラブルシューティング](#)

## MediaPackage のサービスにリンクされたロールの使用

AWS Elemental MediaPackage は、IAM [サービスにリンクされたロール](#) を使用します。サービスにリンクされたロールは、に直接リンクされた一意のタイプの IAM ロールです MediaPackage。サービスにリンクされたロールは、によって事前定義 MediaPackage されており、ユーザーに代わってサービスから他の AWS のサービスを呼び出すために必要なすべてのアクセス許可が含まれています。

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

サービスリンクロールは、まずその関連リソースを削除しなければ削除できません。これにより、MediaPackage リソースにアクセスするためのアクセス許可を誤って削除することがないため、リソースが保護されます。

サービスリンクロールをサポートする他のサービスについては、「[IAM と連携する AWS サービス](#)」で「サービスリンクロール」列が「はい」になっているサービスを探してください。サービスのサービスリンクロールに関するドキュメンテーションを表示するには、[Yes] (はい) リンクを選択します。

## MediaPackage のサービスにリンクされたロールのアクセス許可

MediaPackage は、という名前のサービスにリンクされたロール MediaPackage を使用します AWSServiceRoleForMediaPackage。はこのサービスにリンクされたロール CloudWatch を使用してを呼び出し、ロググループ、ログストリーム、ログイベントを作成および管理します。

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

- `mediapackage.amazonaws.com`

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

- アクション: `arn:aws:logs:*:*:log-group:/aws/MediaPackage/*:log-stream:*` 上で `logs:PutLogEvents`
- アクション: `logs>CreateLogStream`, `logs>CreateLogGroup`, `logs:DescribeLogGroups`, `logs:DescribeLogStreams` 上で `arn:aws:logs:*:*:log-group:/aws/MediaPackage/*`

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

## のサービスにリンクされたロールの作成 MediaPackage

サービスリンクロールを手動で作成する必要はありません。AWS Management Console、AWS CLI または AWS API でアクセスログ記録を有効にすると、MediaPackage によってサービスにリンクされたロールが作成されます。

このサービスリンクロールを削除した後で再度作成する必要がある場合は、同じ方法でアカウントにロールを再作成できます。アクセスログ記録を有効にすると、によってサービスにリンクされたロールが再度 MediaPackage 作成されます。

IAM コンソールを使用して、MediaPackage ユースケースでサービスにリンクされたロールを作成することもできます。AWS CLI または AWS API で、サービス名を使用して `mediapackage.amazonaws.com` サービスにリンクされたロールを作成します。詳細については、「IAM ユーザーガイド」の「[サービスにリンクされたロールの作成](#)」を参照してください。このサービスリンクロールを削除しても、同じ方法でロールを再作成できます。

## のサービスにリンクされたロールの編集 MediaPackage

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

## のサービスにリンクされたロールの削除 MediaPackage

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングさ

れたり、メンテナンスされたりすることがなくなります。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

#### Note

リソースを削除しようとしたときに MediaPackage サービスがロールを使用している場合、削除が失敗する可能性があります。失敗した場合は、数分待ってから操作を再試行してください。

が使用する MediaPackage リソースを削除するには `AWSServiceRoleForMediaPackage`

- AWS Management Console、AWS CLI または AWS API のアクセスログ記録を無効にします。

サービスにリンクされたロールを IAM で手動削除するには

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

MediaPackage のサービスにリンクされたロールをサポートするリージョン

MediaPackage は、サービスが利用可能なすべてのリージョンでサービスにリンクされたロールの使用をサポートします。詳細については、「[AWS リージョンとエンドポイント](#)」を参照してください。

## でのログ記録とモニタリング AWS Elemental MediaPackage

このセクションでは、セキュリティ上の目的で AWS Elemental MediaPackage 内でログ記録およびモニタリングを行うためのオプションについての概要を説明します。でのログ記録とモニタリングの詳細については、MediaPackage 「」を参照してください [でのログ記録とモニタリング AWS Elemental MediaPackage](#)。

モニタリングは、および 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 AWS Elemental MediaPackage 上で重要な部分です。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、AWS ソリューションのすべての部分からモニタリングデータを

収集する必要があります。AWS には、リソースを MediaPackage モニタリングし、潜在的なインシデントに対応するための複数のツールが用意されています。

## Amazon CloudWatch アラーム

CloudWatch アラームを使用すると、指定した期間にわたって 1 つのメトリクスを監視できます。メトリクスが特定のしきい値を超えると、Amazon SNS トピックまたは AWS Auto Scaling policy。CloudWatch alarms は特定の状態にあるため、アクションを呼び出しません。その代わりに、状態が変更され、指定期間にわたって維持される必要があります。詳細については、「[Amazon CloudWatch メトリクス AWS Elemental MediaPackage によるモニタリング](#)」を参照してください。

## AWS CloudTrail ログ

CloudTrail は、 のユーザー、ロール、または AWS のサービスによって実行されたアクションの記録を提供します AWS Elemental MediaPackage。によって収集された情報を使用して CloudTrail、 に対するリクエスト MediaPackage、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。詳細については、「[を使用した AWS Elemental MediaPackage API コーラのログ記録 AWS CloudTrail](#)」を参照してください。

## AWS Elemental MediaPackage アクセスログ

サーバーアクセスログでは、チャンネルに対して行われたリクエストの詳細なレコードが提供されます。サーバーアクセスのログは、多くのアプリケーションに役立ちます。例えば、アクセスのログ情報は、セキュリティやアクセスの監査に役立ちます。詳細については、「[アクセスのログ記録](#)」を参照してください。

## AWS Trusted Advisor

Trusted Advisor は、数十万の AWS お客様にサービスを提供することから学んだベストプラクティスを活用しています。は AWS 環境 Trusted Advisor を検査し、コスト削減、システムの可用性とパフォーマンスの向上、セキュリティギャップの解消に役立つ機会があればレコメンデーションを作成します。AWS のすべてのお客様は、5 つの Trusted Advisor チェックにアクセスできます。ビジネスまたはエンタープライズサポートプランをご利用のお客様は、すべての Trusted Advisor チェックを表示できます。

詳細については、「[AWS Trusted Advisor](#)」を参照してください。



# のコンプライアンス検証 AWS Elemental MediaPackage

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラム [AWS のサービス による対象範囲内のコンプライアンスプログラム](#) を参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、[AWS 「コンプライアンスプログラム」](#) を参照してください。

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

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。では、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- [セキュリティとコンプライアンスのクイックスタートガイド](#) – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- [アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャー](#) – このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

## Note

すべて AWS のサービス HIPAA の対象となるわけではありません。詳細については、[「HIPAA 対応サービスのリファレンス」](#) を参照してください。

- [AWS コンプライアンスリソース](#) – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- [AWS カスタマーコンプライアンスガイド](#) – コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- [「デベロッパーガイド」の「ルールによるリソースの評価」](#) – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。AWS Config



- [AWS Security Hub](#) – これにより AWS のサービス、内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、「[Security Hub のコントロールリファレンス](#)」を参照してください。
- [Amazon GuardDuty](#) — これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービスを検出します。GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件への対応に役立ちます。
- [AWS Audit Manager](#) – これにより AWS のサービス、AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

## の耐障害性 AWS Elemental MediaPackage

AWS グローバルインフラストラクチャは、AWS リージョンとアベイラビリティーゾーンを中心に構築されています。AWS リージョンは、低レイテンシー、高スループット、および冗長性の高いネットワークで接続された、物理的に分離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。

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

## のインフラストラクチャセキュリティ AWS Elemental MediaPackage

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

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

- Transport Layer Security (TLS)。TLS 1.2 は必須で TLS 1.3 がお勧めです。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

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

# でのログ記録とモニタリング AWS Elemental MediaPackage

モニタリングは、AWS Elemental MediaPackage およびその他の AWS ソリューションの信頼性、可用性、およびパフォーマンスを維持する上で重要な部分です。は、をモニタリングし MediaPackage、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。

- Amazon CloudWatch は、AWS リソースと、AWS で実行しているアプリケーションをリアルタイムでモニタリングします。メトリクスを収集および追跡し、カスタマイズされたダッシュボードを作成し、指定されたメトリックが指定したしきい値に達したときに通知またはアクションを実行するアラームを設定できます。例えば、で Amazon EC2 インスタンスの CPU 使用率やその他のメトリクス CloudWatch を追跡し、必要に応じて新しいインスタンスを自動的に起動できます。詳細については、[「Amazon ユーザーガイド CloudWatch」](#)を参照してください。
- Amazon CloudWatch Events は、AWS リソースの変更を記述するシステムイベントのほぼリアルタイムのストリームを提供します。CloudWatch Events は、特定のイベントを監視し、これらのイベントが発生したときに他の AWS のサービスで自動アクションをトリガーするルールを記述できるため、自動イベント駆動型コンピューティングを有効にします。詳細については、[「Amazon CloudWatch Events ユーザーガイド」](#)を参照してください。
- AWS CloudTrail は、AWS アカウントによって、またはアカウントに代わって行われた API コールおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。を呼び出したユーザーとアカウント AWS、呼び出し元の IP アドレス、呼び出しが発生した日時を特定できます。詳細については、[『AWS CloudTrail ユーザーガイド』](#)を参照してください。
- AWS Elemental MediaPackage アクセスログは、チャンネルに対して行われたリクエストに関する詳細レコードを提供します。アクセスのログは、多くのアプリケーションに役立ちます。例えば、アクセスのログ情報は、セキュリティやアクセスの監査に役立ちます。詳細については、[「アクセスのログ記録」](#)を参照してください。
- MediaPackage マニフェスト更新ヘッダーは、動的広告挿入を使用しないワークフローで、サービスがマニフェストとセグメントシーケンスを最後に更新した日時を示します。は、再生レスポンスにこれらのカスタムヘッダー MediaPackage を含めます。これらのヘッダーは、古いマニフェストに関連する問題のトラブルシューティングに役立ちます。詳細については、[「マニフェストの更新時間のモニタリング」](#)を参照してください。

## トピック

- [Amazon CloudWatch メトリクス AWS Elemental MediaPackage によるモニタリング](#)
- [CloudWatch イベント AWS Elemental MediaPackage によるモニタリング](#)
- [を使用した AWS Elemental MediaPackage API コールのログ記録 AWS CloudTrail](#)
- [アクセスのログ記録](#)
- [マニフェストの更新時間のモニタリング](#)
- [ワークフローモニターを使用した AWS メディアサービスのモニタリング](#)

# Amazon CloudWatch メトリクス AWS Elemental MediaPackage によるモニタリング

raw データを収集し CloudWatch、読み取り可能なほぼリアルタイムのメトリクスに処理する AWS Elemental MediaPackage を使用してモニタリングできます。これらの統計は 15 か月間保持されるため、履歴情報にアクセスし、ウェブアプリケーションまたはサービスの動作をよりの確に把握できます。また、特定のしきい値を監視するアラームを設定し、これらのしきい値に達したときに通知を送信したりアクションを実行したりできます。詳細については、「[Amazon ユーザーガイド CloudWatch](#)」を参照してください。

MediaPackage コンソールを使用してメトリクスを表示するには

MediaPackage コンソール全体にメトリクスが表示されます。

1. <https://console.aws.amazon.com/mediapackage/> で MediaPackage コンソールを開きます。
2. メトリクスを表示する適切なページに移動します。
  - のすべてのチャンネルとエンドポイントのメトリクスについては AWS リージョン、「チャンネル」ページを参照してください。
  - 特定のチャンネルとそのチャンネルに含まれるすべてのエンドポイントのメトリクスについては、チャンネルの詳細ページに移動します。
  - 特定のエンドポイントとそのチャンネルのメトリクスについては、エンドポイントの詳細ページに移動します。
3. (オプション) メトリクスビューを絞り込むには、 で開くを選択します CloudWatch。

CloudWatch コンソールを使用してメトリクスを表示するには

メトリクスはまずサービスの名前空間ごとにグループ化され、次に各名前空間内のさまざまなディメンションの組み合わせごとにグループ化されます。

1. にサインイン AWS Management Console し、<https://console.aws.amazon.com/cloudwatch/> で CloudWatch コンソールを開きます。
2. ナビゲーションペインで メトリクスを選択します。
3. すべてのメトリクスで、AWS/MediaPackage 名前空間を選択します。
4. メトリクスディメンションを選択してメトリクスを表示します (たとえば、channel を選択してチャンネル別にメトリクスを表示します)。

を使用してメトリクスを表示するには AWS CLI

コマンドプロンプトで、次のコマンドを使用します。

```
aws cloudwatch list-metrics --namespace "AWS/MediaPackage"
```

トピック

- [AWS Elemental MediaPackage ライブコンテンツメトリクス](#)
- [AWS Elemental MediaPackage VOD コンテンツメトリクス](#)

## AWS Elemental MediaPackage ライブコンテンツメトリクス

AWS/MediaPackage 名前空間には、ライブコンテンツの次のメトリクスが含まれています。は、メトリクスを 1 分 CloudWatch ごとに AWS Elemental MediaPackage 発行します。

メトリクス	説明
ActiveInput	入力が のエンドポイントのソースとして使用されたかどうかを示します MediaPackage (アクティブ)。値が 1 であれば入力がアクティブであったことを示します。0 (ゼロ) の場合はアクティブではなかったことを示します。 単位: なし  有効なディメンション:

メトリクス	説明
EgressBytes	<ul style="list-style-type: none"><li>• IngestEndpoint と OriginEndpoint の組み合わせ</li></ul> <p>が各リクエストに対して MediaPackage 正常に送信したバイト数。MediaPackage が指定された間隔で出力リクエストを受信しない場合、データは提供されません。</p> <p>単位: バイト</p> <p>有効な統計:</p> <ul style="list-style-type: none"><li>• Average – 設定した間隔に AWS Elemental MediaPackage 出力される平均バイト数 (Sum/SampleCount )。</li><li>• Maximum – AWS Elemental MediaPackage に対して発行された個別の出力リクエストの最大サイズ (バイト単位)。</li><li>• Minimum – AWS Elemental MediaPackage に対して発行された個別の出力リクエストの最小サイズ (バイト単位)。</li><li>• SampleCount – 統計の計算で使用するリクエスト数。</li><li>• Sum - 設定した間隔内に AWS Elemental MediaPackage 出力されるバイトの合計数。</li></ul> <p>有効なディメンション:</p> <ul style="list-style-type: none"><li>• Channel</li><li>• Channel と OriginEndpoint の組み合わせ</li><li>• PackagingConfiguration</li><li>• ディメンションなし</li></ul>

メトリクス	説明
EgressRequestCount	<p>が AWS Elemental MediaPackage 受信するコンテンツリクエストの数。MediaPackage が指定された間隔で出力リクエストを受信しない場合、データは提供されません。</p> <p>単位: カウント</p> <p>有効な統計:</p> <ul style="list-style-type: none"><li>• Sum – AWS Elemental MediaPackage での出力リクエストの総受信数。</li></ul> <p>有効なディメンション:</p> <ul style="list-style-type: none"><li>• Channel</li><li>• Channel と OriginEndpoint の組み合わせ</li><li>• StatusCodeRange</li><li>• Channel と StatusCodeRange の組み合わせ</li><li>• Channel、OriginEndpoint、および StatusCodeRange の組み合わせ</li><li>• PackagingConfiguration</li><li>• PackagingConfiguration と StatusCodeRange の組み合わせ</li><li>• ディメンションなし</li></ul>



メトリクス	説明
EgressResponseTime	<p>各出力リクエストの処理 MediaPackage にかかる時間。MediaPackage が指定された間隔で出力リクエストを受信しない場合、データは提供されません。</p> <p>単位: ミリ秒</p> <p>有効な統計:</p> <ul style="list-style-type: none"><li>• Average – 設定した間隔における出力リクエストの処理 AWS Elemental MediaPackage にかかる平均時間 (Sum/SampleCount )。</li><li>• Maximum – AWS Elemental MediaPackage が出力リクエストを処理してレスポンスを提供する最長所要時間 (ミリ秒単位)。</li><li>• Minimum – 出力リクエストを処理してレスポンスを提供する AWS Elemental MediaPackage のにかかる最短時間 (ミリ秒単位)。</li><li>• SampleCount – 統計の計算で使用するリクエスト数。</li><li>• Sum - 設定した間隔内に出力リクエストを処理する AWS Elemental MediaPackage のにかかる合計時間。</li></ul> <p>有効なディメンション:</p> <ul style="list-style-type: none"><li>• Channel</li><li>• Channel と OriginEndpoint の組み合わせ</li><li>• PackagingConfiguration</li></ul>

メトリクス	説明
IngressBytes	<p>が入力リクエストごとに AWS Elemental MediaPackage 受信するコンテンツのバイト数。MediaPackage が指定された間隔で入力リクエストを受信しない場合、データは提供されません。</p> <p>単位: バイト</p> <p>有効な統計:</p> <ul style="list-style-type: none"><li>• Average - が設定した間隔内に MediaPackage 受信する平均バイト数 (Sum/SampleCount )。</li><li>• Maximum – AWS Elemental MediaPackage に対して発行された個別の入力リクエストの最大サイズ (バイト単位)。</li><li>• Minimum – AWS Elemental MediaPackage に対して発行された個別の入力リクエストの最小サイズ (バイト単位)。</li><li>• SampleCount – 統計の計算で使用するリクエスト数。</li><li>• Sum - が設定した間隔内に AWS Elemental MediaPackage 受信する合計バイト数。</li></ul> <p>有効なディメンション:</p> <ul style="list-style-type: none"><li>• Channel</li><li>• Channel と IngestEndpoint の組み合わせ</li><li>• ディメンションなし</li></ul>

メトリクス	説明
IngressResponseTime	<p>各入力リクエストの処理 MediaPackage にかかる時間。MediaPackage が指定された間隔で入力リクエストを受信しない場合、データは提供されません。</p> <p>単位: ミリ秒</p> <p>有効な統計:</p> <ul style="list-style-type: none"> <li>• Average – 設定された間隔における入力リクエストの処理 MediaPackage にかかる平均時間 (Sum/SampleCount )。</li> <li>• Maximum – AWS Elemental MediaPackage が入力リクエストを処理してレスポンスを提供する最長所要時間 (ミリ秒単位)。</li> <li>• Minimum – 入力リクエストを処理してレスポンスを提供する AWS Elemental MediaPackage のにかかる最短時間 (ミリ秒単位)。</li> <li>• SampleCount – 統計の計算で使用するリクエスト数。</li> <li>• Sum - 設定した間隔内に入力リクエストを処理する MediaPackage のにかかる合計時間。</li> </ul> <p>有効なディメンション:</p> <ul style="list-style-type: none"> <li>• Channel</li> <li>• Channel と IngestEndpoint の組み合わせ</li> <li>• ディメンションなし</li> </ul>

## AWS Elemental MediaPackage ライブディメンション

以下のディメンションを使用して AWS/MediaPackage データをフィルタリングできます。

ディメンション	説明
ディメンションなし	すべてのチャンネル、エンドポイント、またはステータスコードのメトリクスが集約されて表示されます。
Channel	<p>指定したチャンネルのメトリクスのみが表示されます。</p> <p>値: チャンネルの自動生成された GUID。</p> <p>単独で使用するか、他のディメンションと組み合わせて使用できます。</p> <ul style="list-style-type: none"><li>• 単独で使用する、指定したチャンネルのみのメトリクスが表示されます。</li><li>• <code>originEndpoint</code> ディメンションと組み合わせて使用すると、指定したチャンネルに関連付けられている指定したエンドポイントのメトリクスが表示されます。</li></ul>
IngestEndpoint	<p>チャンネルで指定したインGESTエンドポイントのみのメトリクスが表示されます。</p> <p>値: インGESTエンドポイントの自動生成された GUID。</p> <p>次のディメンションで使用できます。</p> <ul style="list-style-type: none"><li>• <code>channel</code> ディメンションと組み合わせて使用すると、指定したチャンネルに関連付けられている指定したインGESTエンドポイントのメトリクスが表示されます。</li><li>• <code>originEndpoint</code> ディメンションと組み合わせて使用すると、指定したエンドポイントに関連付けられている指定したインGESTエンドポイントのメトリクスが表示されます。</li></ul>

ディメンション	説明
OriginEndpoint	<p>指定したチャンネルとエンドポイントの組み合わせのメトリクスが表示されます。</p> <p>値: エンドポイントの自動生成された GUID。</p> <p>channel ディメンションと組み合わせて使用する必要があります。</p>
StatusCodeRange	<p>指定したステータスコード範囲のメトリクスが表示されます。</p> <p>値: 2xx、3xx、4xx、または 5xx。</p> <p>単独で使用するか、他のディメンションと組み合わせて使用できます。</p> <ul style="list-style-type: none"> <li>単独で使用する、指定したステータス範囲のすべての出力リクエストが表示されます。</li> <li>channel ディメンションと組み合わせて使用すると、指定したチャンネルに関連付けられた、指定したステータスコード範囲のすべてのエンドポイントの出力リクエストが表示されます。</li> <li>channel ディメンションおよび originEndpoint ディメンションと組み合わせて使用すると、指定したチャンネルに関連付けられている指定したエンドポイントの特定のステータスコード範囲の出力リクエストが表示されます。</li> </ul>

## AWS Elemental MediaPackage VOD コンテンツメトリクス

AWS/MediaPackage 名前空間には、ビデオオンデマンド (VOD) コンテンツの次のメトリクスが含まれています。は、メトリクスを 1 分 CloudWatch ごとに AWS Elemental MediaPackage 発行します。

メトリクス	説明
EgressBytes	<p>が各リクエストに対して MediaPackage 正常に送信したバイト数。MediaPackage が指定された間隔で出力リクエストを受信しない場合、データは提供されません。</p> <p>単位: バイト</p> <p>有効な統計:</p> <ul style="list-style-type: none"><li>• Average – 設定した間隔に MediaPackage 出力される平均バイト数 (Sum/SampleCount )。</li><li>• Maximum – に対して行われた個々の出力リクエストの最大数 (バイト単位) MediaPackage。</li><li>• Minimum – に対して行われた個々の出力リクエストの最小サイズ (バイト単位) MediaPackage。</li><li>• SampleCount – 統計の計算で使用するリクエスト数。</li><li>• Sum - 設定した間隔で MediaPackage 出力されるバイトの合計数。</li></ul> <p>有効なディメンション:</p> <ul style="list-style-type: none"><li>• PackagingConfiguration</li></ul>
EgressRequestCount	<p>が MediaPackage 受信するコンテンツリクエストの数。MediaPackage が指定された間隔で出力リクエストを受信しない場合、データは提供されません。</p> <p>単位: カウント</p> <p>有効な統計:</p>

メトリクス	説明
	<ul style="list-style-type: none"> <li>Sum - が MediaPackage受信した出力リクエストの合計数。</li> </ul> <p>有効なディメンション:</p> <ul style="list-style-type: none"> <li>PackagingConfiguration</li> <li>PackagingConfiguration と StatusCodeRange の組み合わせ</li> </ul>
EgressResponseTime	<p>各出力リクエストの処理 MediaPackage にかかる時間。MediaPackage が指定された間隔で出力リクエストを受信しない場合、データは提供されません。</p> <p>単位: ミリ秒</p> <p>有効な統計:</p> <ul style="list-style-type: none"> <li>Average - 設定した間隔における出力リクエストの処理 MediaPackage にかかる平均時間 (Sum/SampleCount )。</li> <li>Maximum - 出力リクエストを処理し MediaPackage でレスポンスを提供するのにかかる最長時間 (ミリ秒単位)。</li> <li>Minimum - 出力リクエストを処理してレスポンスを提供する MediaPackage のにかかる最短時間 (ミリ秒単位)。</li> <li>SampleCount - 統計の計算で使用するリクエスト数。</li> <li>Sum - 設定した間隔内に出力リクエストを処理する MediaPackage のにかかる合計時間。</li> </ul> <p>有効なディメンション:</p> <ul style="list-style-type: none"> <li>PackagingConfiguration</li> </ul>



## AWS Elemental MediaPackage VOD デイメンション

以下のデイメンションを使用して AWS/MediaPackage データをフィルタリングできます。

デイメンション	説明
デイメンションなし	メトリクスはすべてのパッケージ設定とステータスコードについて集約されて表示されます。
PackagingConfiguration	<p>メトリクスは、指定されたパッケージ設定に対してのみ表示されます。</p> <p>値: 設定の自動生成された GUID。</p> <p>単独で使用するか、他のデイメンションと組み合わせて使用できます。</p> <ul style="list-style-type: none"> <li>単独で使用すると、指定した設定のみのメトリクスが表示されます。</li> <li>statusCodeRange デイメンションと組み合わせて使用すると、指定したステータスコードに関連付けられている指定した設定のメトリクスが表示されます。</li> </ul>
StatusCodeRange	<p>指定したステータスコード範囲のメトリクスが表示されます。</p> <p>値: 2xx、3xx、4xx、または 5xx。</p> <p>単独で使用するか、他のデイメンションと組み合わせて使用できます。</p> <ul style="list-style-type: none"> <li>単独で使用すると、指定したステータス範囲のすべての出力リクエストが表示されます。</li> <li>channel デイメンションと組み合わせて使用すると、指定したチャンネルに関連付けられた、指定したステータスコード範囲のすべてのエンドポイントの出力リクエストが表示されます。</li> </ul>

ディメンション	説明
	<ul style="list-style-type: none"><li>• channel ディメンションおよび originEndpoint ディメンションと組み合わせて使用すると、指定したチャンネルに関連付けられている指定したエンドポイントの特定のステータスコード範囲の出力リクエストが表示されます。</li></ul>

## CloudWatch イベント AWS Elemental MediaPackage によるモニタリング

Amazon CloudWatch Events を使用すると、AWS サービスを自動化し、アプリケーションの可用性の問題やエラー条件などのシステムイベントに自動的に対応できます。AWS サービスは、イベントをほぼリアルタイムで CloudWatch イベントに配信します。簡単なルールを記述して、注目するイベントと、イベントがルールに一致した場合に自動的に実行するアクションを指定できます。自動的にトリガーできるオペレーションには、以下が含まれます。

- AWS Lambda 関数の呼び出し
- AWS Systems Manager Run Command の呼び出し
- Amazon Kinesis Data Streams へのイベントの中継
- AWS Step Functions ステートマシンのアクティブ化

で CloudWatch Events を使用する例としては、ストリーム入力の最大数に達した場合の Amazon SNS トピックの通知があります。MediaPackage は、ベストエフォートベースで MediaPackage イベントを発行します。

Events でのルールの作成の詳細については、CloudWatch [「Amazon CloudWatch Events ユーザーガイド」](#)を参照してください。

が発行するイベントのリストについては、MediaPackage [「」](#)を参照してください [AWS Elemental MediaPackage イベント](#)。

## AWS Elemental MediaPackage イベント

AWS Elemental MediaPackage は Amazon CloudWatch Events と統合して、チャンネルやエンドポイントに影響する特定のイベントを通知します。各イベントは [JSON \(JavaScript Object Notation\)](#) で表され、イベント名、イベントが発生した日時、影響を受けるチャンネルまたはエンドポイント、およびベストエフォートベースでイベント MediaPackage を発行します。CloudWatch Events を使用してこれらのイベントを収集し、AWS Lambda 関数、Amazon SNS トピック、Amazon SQS キュー、Amazon Kinesis Data Streams のストリーム、組み込みターゲットなどの 1 つ以上のターゲットにルーティングするルールを設定できます。

他の種類の CloudWatch イベントでイベントを使用する方法の詳細については、[「Amazon CloudWatch Events ユーザーガイド」](#) を参照してください。

以下のトピックでは、が MediaPackage 作成する CloudWatch イベントについて説明します。

### イベントタイプ

- [入力通知イベント](#)
- [キープロバイダーの通知イベント](#)
- [収集ジョブの通知イベント](#)

### 入力通知イベント

ライブおよびビデオオンデマンド (VOD) コンテンツの入力通知イベントを取得します。これらのイベントは、MediaPackage 取り込みで何かが発生したときに通知します。以下は、受け取る可能性のある入力通知イベントです。

- 最大入カストリームの超過
- 入カスイッチ
- VOD 取り込みステータスの変更
- VOD 再生の準備完了

以下のセクションでは、これらの各イベントについて説明します。

## 最大入力ストリーム超過イベント

ライブコンテンツの場合、のチャンネルは入力ストリーム数のクォータ MediaPackage を超えています。クォータの詳細については、「[AWS Elemental MediaPackage のクォータ](#)」を参照してください。

### Example

```
{
  "id": "7bf73129-1428-4cd3-a780-95db273d1602",
  "detail-type": "MediaPackage Input Notification",
  "source": "aws.mediapackage",
  "account": "aws_account_id",
  "time": "2015-11-11T21:29:54Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:mediapackage:us-west-2:aws_account_id:channels/262ff182d46d4b399fcabea1364df682"
  ],
  "detail": {
    "event": "MaxIngestStreamsError",
    "message": "Parent Manifest [%s] has [23] streams, more than [20] allowed:
(index_1.m3u8,index_2.m3u8,index_3.m3u8,index_4.m3u8,index_5.m3u8,index_6.m3u8,index_7.m3u8"
  }
}
```

## 入力切り替えイベント

ライブコンテンツの場合、はいずれかのエンドポイントの入力を MediaPackage 切り替えます。

1つのイベントは5分間隔で送信されます。入力が5分間に複数回切り替わった場合(例えば、が1つの入力に MediaPackage 切り替わり、次に別の入力に戻る場合)、受信するイベントは1つだけです。

入力冗長およびどのような場合に入力が切り替えられるかについては、「[ライブ入力冗長の AWS Elemental MediaPackage 処理の流れ](#)」を参照してください。

### Example

```
{
  "id": "8f9b8e72-0b31-e883-f19c-aec84742f3ce",
  "detail-type": "MediaPackage Input Notification",
```

```

"source": "aws.mediapackage",
"account": "aws_account_id",
"time": "2018-07-16T17:29:36Z",
"region": "us-east-1",
"resources": [
  "arn:aws:mediapackage:us-east-1:aws_account_id:origin_endpoints/82d6b9bc04cb4612b487963d6c8d0f1a"
],
"detail": {
  "event": "InputSwitchEvent",
  "message": "Origin endpoint experienced an Input Switch Event",
  "EventDetails": {
    "Channel": "channel name",
    "PreviousIngestEndpoint": "endpoint uuid before input switch",
    "CurrentIngestEndpoint": "endpoint uuid after input switch",
  }
}
}

```

## VOD 取り込みステータスイベント

ビデオオンデマンド (VOD) コンテンツの場合、のアセットは取り込みステータス MediaPackage を変更します。以下のイベントの通知を受け取ります。

- IngestStart
- IngestError
- IngestComplete

### Example

```

{
  "id": "8f9b8e72-0b31-e883-f19c-aec84742f3ce",
  "detail-type": "MediaPackage Input Notification",
  "source": "aws.mediapackage",
  "account": "aws_account_id",
  "time": "2019-05-03T17:29:36Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:mediapackage-vod:us-west-2:aws_account_id:assets/asset_name"
  ],
  "detail": {

```

```
    "event": "IngestComplete",
    "message": "message text"
  }
}
```

## VOD 再生イベント

VOD コンテンツの場合、のアセット MediaPackage を再生できます。アセットの取り込みが完了してから、アセットが再生可能になるまでに時間がかかります。イベント VodAssetPlayable は、アセットの再生リクエストを処理 MediaPackage できることを意味します。

パッケージンググループ内の各パッケージング設定について、個別の VodAssetPlayable イベントを取得することができます。例えば、パッケージンググループに DASH と HLS のパッケージング設定が各 1 つずつ含まれている場合は、ユーザーは (DASH パッケージング設定用と HLS パッケージング設定用として) 2 つの VodAssetPlayable イベントを受け取ります。

### Example

```
{
  "id": "81e896e4-d9e5-ec79-f82a-b4cf3246c567",
  "detail-type": "MediaPackage Input Notification",
  "source": "aws.mediapackage",
  "account": "aws_account_id",
  "time": "2019-11-03T21:46:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:mediapackage-vod:us-west-2:aws_account_id:assets/asset_id",
    "arn:aws:mediapackage-vod:us-west-2:aws_account_id:packaging_configuration/packaging_configuration_id"
  ],
  "detail": {
    "event": "VodAssetPlayable",
    "message": "Asset 'asset_id' is now playable for PackagingConfiguration 'packaging_configuration_id'",
    "packaging_configuration_id": "packaging_configuration_id",
    "manifest_urls": [
      "https://555555555555.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/b9cc115bf7f1a/b848dfb116920772aa69ba/a3c74b1cae6a451c/index.m3u8"
    ]
  }
}
```

```
{
  "id": "91e896e4-d9e5-ab80-f82a-b4cf3246c568",
  "detail-type": "MediaPackage Input Notification",
  "source": "aws.mediapackage",
  "account": "aws_account_id",
  "time": "2019-11-03T21:47:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:mediapackage-vod:us-west-2:aws_account_id:assets/asset_id",
    "arn:aws:mediapackage-vod:us-
west-2:aws_account_id:packaging_configuration/packaging_configuration_id"
  ],
  "detail": {
    "event": "VodAssetPlayable",
    "message": "Asset 'asset_id' is now playable for PackagingConfiguration
'packaging_configuration_id'",
    "packaging_configuration_id": "packaging_configuration_id",
    "manifest_urls": [
      "https://111122223333.egress.mediapackage-vod.us-west-2.amazonaws.com/out/
v1/1234567890abc/021345abcdef6789012345/abcdef0123456789/index.mpd"
    ]
  }
}
```

## キープロバイダーの通知イベント

エンドポイントでコンテンツ暗号化を使用していて、キープロバイダーに到達 MediaPackage できない場合、キープロバイダー通知イベントが発生します。DRM と暗号化の詳細については、<https://docs.aws.amazon.com/speke/latest/documentation/> を参照してください。

### Example ライブキープロバイダー通知イベント

```
{
  "id": "7bf73129-1428-4cd3-a780-98ds273d1602",
  "detail-type": "MediaPackage Key Provider Notification",
  "source": "aws.mediapackage",
  "account": "aws_account_id",
  "time": "2015-11-11T21:29:54Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:mediapackage:us-west-2:aws_account_id:origin_endpoints/endpoint_id"
  ]
}
```



```
  ],
  "detail":{
    "event": "KeyProviderError",
    "message": "message-text"
  }
}
```

### Example VOD キープロバイダー通知イベント

```
{
  "id": "7bf73129-1428-4cd3-a780-98ds273d1602",
  "detail-type": "MediaPackage Key Provider Notification",
  "source": "aws.mediapackage",
  "account": "aws_account_id",
  "time": "2015-11-11T21:29:54Z",
  "region": "us-west-2",
  "resources":[
    "arn:aws:mediapackage-vod:us-west-2:aws_account_id:packaging_configurations/packaging_group_name"
  ],
  "detail":{
    "event": "KeyProviderError",
    "message": "message-text"
  }
}
```

### 収集ジョブの通知イベント

ライブストリームからクリップをエクスポートして Live-to-VOD アセットを作成すると、収集ジョブのステータスイベントが発生します。は、収集ジョブが成功または失敗したときに通知 MediaPackage を作成します。収集ジョブと live-to-VOD アセットについては、「[AWS Elemental MediaPackage を使用した live-to-VOD アセットの作成](#)」を参照してください。

### Example 成功した収集ジョブのイベント

```
{
  "id": "8f9b8e72-0b31-e883-f19c-aec84742f3ce",
  "detail-type": "MediaPackage HarvestJob Notification",
  "source": "aws.mediapackage",
  "account": "aws_account_id",
  "time": "2019-07-16T17:29:36Z",
  "region": "us-east-1",
```

```

"resources": [
  "arn:aws:mediapackage:us-east-1:aws_account_id:harvest_jobs/harvest_job_id"
],
"detail": {
  "harvest_job": {
    "id": "harvest_job_id",
    "arn": "arn:aws:mediapackage-vod:us-east-1:aws_account_id:harvest_jobs/harvest_job_id",
    "status": "SUCCEEDED",
    "origin_endpoint_id": "endpoint_id",
    "start_time": "2019-06-26T20:30:00-08:00",
    "end_time": "2019-06-26T21:00:00-08:00",
    "s3_destination": {
      "bucket_name": "s3_bucket_name",
      "manifest_key": "path/and/manifest_name/index.m3u8",
      "role_arn": "arn:aws:iam::aws_account_id:role/S3Access_role",
    },
    "created_at": "2019-06-26T21:03:12-08:00"
  }
}
}

```

### Example 失敗した収集ジョブのイベント

```

{
  "id": "8f9b8e72-0b31-e883-f19c-aec84742f3ce",
  "detail-type": "MediaPackage HarvestJob Notification",
  "source": "aws.mediapackage",
  "account": "aws_account_id",
  "time": "2019-07-16T17:29:36Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:mediapackage:us-east-1:aws_account_id:harvest_jobs/harvest_job_id"
  ],
  "detail": {
    "harvest_job": {
      "id": "harvest_job_id",
      "arn": "arn:aws:mediapackage-vod:us-east-1:aws_account_id:harvest_jobs/harvest_job_id",
      "status": "FAILED",
      "origin_endpoint_id": "endpoint_id",
      "start_time": "2019-06-26T20:30:00-08:00",
      "end_time": "2019-06-26T21:00:00-08:00",
    }
  }
}

```

```
    "s3_destination": {
      "bucket_name": "s3_bucket_name",
      "manifest_key": "path/and/manifest_name/index.m3u8",
      "role_arn": "arn:aws:iam::aws_account_id:role/S3Access_role",
    },
    "created_at": "2019-06-26T21:03:12-08:00"
  },
  "message": "Message text"
}
}
```

## イベント通知の作成

Amazon CloudWatch Events と Amazon Simple Notification Service (Amazon SNS) を使用して、新しいイベントを通知できます。CloudWatch イベントでは、通知されるイベントがルールで記述されます。Amazon SNS では、受け取る通知の種類をトピックで記述します。このセクションでは、からのイベントのトピックとルールを作成するための大まかな手順について説明します AWS Elemental MediaPackage。トピックとルールの詳細については、次のトピックを参照してください。

- [Amazon Simple Notification Service デベロッパーガイドの「トピックを作成する」](#) および [トピックにサブスクライブする](#)」を参照してください。
- [Amazon CloudWatch Events ユーザーガイドの「Amazon CloudWatch Events の開始方法」](#)

CloudWatch イベントの通知を作成するには

1. [Amazon SNS](#) にアクセスし、トピックを作成します。わかりやすく、後で認識できるような名前をトピックに付けます。
2. 作成したトピックにサブスクライブします。受け取る通知の種類と、通知の送信先を選択します。たとえば、E メール通知の場合、[E メール] プロトコルを選択し、エンドポイントで通知を受け取る E メールアドレスを入力します。
3. [CloudWatch イベント](#) にアクセスし、カスタムイベントパターン を使用するルールを作成します。パターンのプレビュー領域で、次のように入力します。

```
{
  "source": [
    "aws.mediapackage"
  ],
  "detail-type": [
```

```
"detail-type from event"  
]  
}
```

detail-type で、イベントから detail-type フィールドに値を入力します。詳細タイプには次の値を使用できます。

- **MediaPackage Input Notification**
- **MediaPackage Key Provider Notification**

イベントタイプについての詳細は、「[AWS Elemental MediaPackage イベント](#)」を参照してください。

#### Example

次のルールの例は、すべての詳細タイプのすべてのイベントの通知を作成します。

```
{  
  "source": [  
    "aws.mediapackage"  
  ],  
  "detail-type": [  
    "MediaPackage Input Notification",  
    "MediaPackage Key Provider Notification",  
    "MediaPackage HarvestJob Notification"  
  ]  
}
```

4. 作成したルールにターゲットを追加します。[SNS トピック] を選択してから、ステップ 1 で作成したトピックを選択します。
5. ルールの詳細を設定し、わかりやすい名前を付けます。ルールの使用を開始するには、有効になっていることを確認してからルールを保存します。

## を使用した AWS Elemental MediaPackage API コールのログ記録 AWS CloudTrail

ログ記録は、 のライブワークフローでのみ使用できます AWS Elemental MediaPackage。

MediaPackage はと統合されています。これは AWS CloudTrail、ユーザー、ロール、またはのサービスによって実行されたアクションを記録する AWS サービスです MediaPackage。は、のすべての API コールをイベント MediaPackage として CloudTrail キャプチャします。これには、MediaPackage コンソールからの呼び出しと MediaPackage API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、の CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます MediaPackage。証跡を設定しない場合でも、CloudTrail コンソールのイベント履歴で最新のイベントを表示できます。によって収集された情報を使用して CloudTrail、に対して行われたリクエスト MediaPackage、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

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

## AWS Elemental MediaPackage の情報 CloudTrail

CloudTrail AWS アカウントを作成すると、がアカウントで有効になります。でアクティビティが発生すると AWS Elemental MediaPackage、そのアクティビティは CloudTrail イベント履歴の他の AWS サービスイベントとともにイベントに記録されます。アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、「[イベント履歴を含む CloudTrail イベントの表示](#)」を参照してください。

のイベントなど、アカウント内のイベントの継続的な記録については MediaPackage、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 AWS リージョン内のすべての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 ログで収集されたイベントデータをより詳細に分析し、それに基づいて行動するように、他の AWS サービスを設定できます。詳細については、次を参照してください:

- [「証跡作成の概要」](#)
- [CloudTrail がサポートするサービスと統合](#)
- [の Amazon SNS 通知の設定 CloudTrail](#)
- [複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからの CloudTrail ログファイルの受信](#)

すべての MediaPackage アクションはによってログに記録 CloudTrail され、[AWS Elemental MediaPackage API リファレンス](#)に記載されています。例えば、CreateChannel、および

RotateIngestEndpointCredentialsオペレーションを呼び出すとCreateOriginEndpoint、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、ルートユーザーまたは IAM ユーザーのどちらの認証情報を使用して送信されたかどうか
- リクエストが、ロールとフェデレーテッドユーザーのどちらの一時的なセキュリティ認証情報を使用して送信されたか
- 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 要素](#)を参照してください。

## AWS Elemental MediaPackage ログファイルエントリについて

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントは任意のソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどに関する情報が含まれます。CloudTrail ログファイルはパブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、UpdateChannelオペレーションを示す CloudTrail ログエントリを示しています。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ABCDEFGHijkl123456789",
    "arn": "arn:aws:sts::444455556666:assumed-role/Admin/testUser",
    "accountId": "444455556666",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-12-18T00:50:58Z"
      }
    },
    "sessionIssuer": {
      "type": "Role",
      "principalId": "ABCDEFGHijkl123456789",
      "arn": "arn:aws:iam::444455556666:role/Admin",
```

```
        "accountId": "444455556666",
        "userName": "Admin"
    }
},
"eventTime": "2018-12-18T00:50:59Z",
"eventSource": "mediapackage.amazonaws.com",
"eventName": "UpdateChannel",
"awsRegion": "us-west-2",
"sourceIPAddress": "203.0.113.17",
"userAgent": "aws-cli/1.15.71 Python/3.6.5 Darwin/17.7.0 botocore/1.10.70",
"requestParameters": {
    "description": "updated cloudtrail description",
    "id": "cloudtrail-test"
},
"responseElements": {
    "description": "updated cloudtrail description",
    "hlsIngest": {
        "ingestEndpoints": [
            {
                "username": "****",
                "url": "https://mediapackage.us-west-2.amazonaws.com/in/
v2/8d0ca97840d94b18b37ad292c131bcad/8d0ca97840d94b18b37ad292c131bcad/channel",
                "password": "****",
                "id": "8d0ca97840d94b18b37ad292c131bcad"
            },
            {
                "username": "****",
                "url": "https://mediapackage.us-west-2.amazonaws.com/in/
v2/8d0ca97840d94b18b37ad292c131bcad/9c17f979598543b9be24345d63b3ad30/channel",
                "password": "****",
                "id": "9c17f979598543b9be24345d63b3ad30"
            }
        ]
    },
    "id": "cloudtrail-test",
    "arn": "arn:aws:mediapackage:us-
west-2:444455556666:channels/8d0ca97840d94b18b37ad292c131bcad"
},
"requestID": "fc158262-025e-11e9-8360-6bff705fbba5",
"eventID": "e9016b49-9a0a-4256-b684-eed9bd9073ab",
"readOnly": false,
"eventType": "AwsApiCall",
"recipientAccountId": "444455556666"
```



```
}
```

## アクセスのログ記録

MediaPackage は、MediaPackage チャンネルまたはパッケージンググループに送信されるリクエストについての詳細情報をキャプチャした、アクセスログを提供します。MediaPackage は、チャンネルの入力エンドポイントに送信されたリクエストに関する、受信アクセスログを生成します。同時に、チャンネルのエンドポイントまたはパッケージンググループのアセットに送信されたリクエストについては、送信アクセスログを生成します。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。これらのアクセスログを使用して、サービスのパフォーマンスを分析し、問題のトラブルシューティングが行えます。また、顧客基盤について調べたり、MediaPackage の請求を把握したりする際にも役立ちます。

アクセスログ記録は、MediaPackage のオプション機能であり、デフォルトでは無効化されています。アクセスのログ記録を有効にすると、MediaPackage はログのキャプチャを開始し、作成または管理時に指定した CloudWatch のロググループに、そのログ記録を保存します。CloudWatch Logs の一般料金が適用されます。

### トピック

- [CloudWatch にログを発行するためのアクセス許可](#)
- [アクセスログの作成の有効化](#)
- [アクセスログの作成の無効化](#)
- [アクセスログの形式](#)
- [アクセスログを読み取る](#)

## CloudWatch にログを発行するためのアクセス許可

アクセスログ記録を有効にすると、MediaPackage は IAM のサービスにリンクされたロール (AWSServiceRoleForMediaPackage) を、AWS アカウント内に作成します。このロールにより、MediaPackage はアクセスログを CloudWatch に公開できるようになります。MediaPackage によるサービスにリンクされたロールの使用については、「[MediaPackage のサービスにリンクされたロールの使用](#)」を参照してください。

## アクセスログの作成の有効化

AWS Management Console または AWS CLI を使用して、アクセスログを有効にできます。

コンソールを使用して既存のチャンネルのアクセスログを有効にするには

1. MediaPackage コンソール (<https://console.aws.amazon.com/mediapackage/>) を開きます。
2. 使用しているチャンネルを選択します。
3. [Configure Access Logs] (アクセスログの設定) セクションで、以下の操作を行います。
  - a. [Enable ingress access logs] (受信アクセスログの有効化) または [Enable egress access logs] (送信アクセスログの有効化) のどちらか (あるいはその両方) を選択します。
  - b. CloudWatch ロググループ名をカスタムで指定できます。この設定を空白のままにすると、デフォルトのグループが使用されます。

コンソールを使用して既存のパッケージンググループのアクセスログを有効にするには

1. MediaPackage コンソール (<https://console.aws.amazon.com/mediapackage/>) を開きます。
2. ナビゲーションセクションで、[Packaging groups] (パッケージンググループ) をクリックします。
3. 使用しているパッケージンググループを選択します。
  - a. ナビゲーションバーで [Edit] (編集) をクリックします。
  - b. [Access logging] (アクセスログ記録) セクションで、[Enable egress access logs] (送信アクセスログの有効化) を選択します。
  - c. CloudWatch ロググループ名をカスタムで指定できます。この設定を空白のままにすると、デフォルトのグループが使用されます。
4. [Save changes] (変更の保存) をクリックします。

AWS CLI を使用してチャンネルのアクセスログを有効にするには

--ingress-access-logs パラメータか --egress-access-logs パラメータ (またはその両方) を指定して [configure-logs](#) コマンドを実行し、アクセスログ記録を有効化します。--ingress-access-logs および --egress-access-logs パラメータには、CloudWatch ロググループ名を含めることができます。ロググループ名を指定しない場合、MediaPackage はデフォルトのロググループを使用します。デフォルトのロググループは、入力ログでは /aws/MediaPackage/IngressAccessLogs に、出力ログの場合は /aws/MediaPackage/EgressAccessLogs になります。

次のコマンドによりデフォルトのロググループを使用して、受信ログとアクセスログの両方を有効化します。

```
aws mediapackage configure-logs --id channel-name --ingress-access-logs {} --egress-access-logs {}
```

このコマンドの戻り値はありません。

AWS CLI を使用してパッケージンググループのアクセスログを有効にするには

--egress-access-logs パラメータを使用して [configure-logs](#) コマンドを実行し、アクセスログ記録を有効にします。--egress-access-logs パラメータには、CloudWatch のロググループ名を含めることができます。ロググループ名を指定しない場合、MediaPackage はデフォルトのロググループを使用します。デフォルトのロググループは、入力ログでは /aws/MediaPackage/IngressAccessLogs に、出力ログの場合は /aws/MediaPackage/EgressAccessLogs になります。

次のコマンドによりデフォルトのロググループを使用して、送信アクセスログを有効化します。

```
aws mediapackage configure-logs --id package-name --egress-access-logs {}
```

このコマンドの戻り値はありません。

## アクセスログの作成の無効化

MediaPackage チャンネルまたはパッケージンググループのアクセスログは、任意のタイミングで無効化できます。

コンソールを使用してアクセスログの作成を無効にするには

1. MediaPackage コンソール (<https://console.aws.amazon.com/mediapackage/>) を開きます。  
チャンネルまたはパッケージンググループを選択します。
2. [Edit] (編集) を選択します。
3. [Access logging] (アクセスログ記録) セクションで、[Ingress access logging] (受信アクセスログ記録) か [Egress access logging] (送信アクセスログ記録) のどちらか (または両方) の選択を解除します。
4. [Save changes] (変更の保存) をクリックします。

AWS CLI を使用してチャンネルのアクセスログ記録を無効にするには

アクセスのログ記録を無効にするには、`configure-logs` コマンドを使用します。`configure-logs` コマンドに、宣言されていないアクセスログパラメータが 1 つ以上存在する場合、それらと対応するアクセスログは無効になります。次のコマンド例では、チャンネルに対して送信アクセスログが有効化され、受信アクセスログは無効化されます。

```
aws mediapackage configure-logs --id channel-name --egress-access-logs {}
```

このコマンドの戻り値はありません。

AWS CLI を使用してパッケージンググループのアクセスログ記録を無効にするには

アクセスのログ記録を無効にするには、`configure-logs` コマンドを使用します。`configure-logs` コマンドに、宣言されていないアクセスログパラメータが 1 つ以上存在する場合、それらと対応するアクセスログは無効になります。例えば、以下のコマンドでは `configure-logs` に `--egress-access-logs` が含まれていないため、送信ログが無効になります。

```
aws mediapackage configure-logs --id package-group-name
```

このコマンドの戻り値はありません。

## アクセスログの形式

アクセスログファイルは、一連の JSON 形式のログレコードで構成されており、各ログレコードは 1 つのリクエストを表します。ログ内のフィールドの順序は変わることがあります。チャンネルでの送信アクセスログの例を次に示します。

```
{
  "timestamp": "2020-07-13T18:59:56.293656Z",
  "clientIp": "192.0.2.0/24",
  "processingTime": 0.445,
  "statusCode": "200",
  "receivedBytes": 468,
  "sentBytes": 2587370,
  "method": "GET",
  "request": "https://aaabbbcccddee.mediapackage.us-east-1.amazonaws.com:443/out/v1/75ee4f20e5df43e5821e5cb17ea19238/hls_7_145095.ts?m=1538005779",
  "protocol": "HTTP/1.1",
```

```
"userAgent": "sabr/3.0 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US)
AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Safari/528.17",
"account": "111122223333",
"channelId": "my_channel",
"channelArn": "arn:aws:mediapackage:us-west-2:111122223333:channels/
ExampleChannelID",
"domainName": "aaabbbcccdddee.mediapackage.us-east-1.amazonaws.com",
"requestId": "aaaAAA111bbbBBB222cccCCC333dddDDD",
"endpointId": "my_endpoint",
"endpointArn": "arn:aws:mediapackage:us-west-2:111122223333:origin_endpoints/
ExampleEndpointID"
}
```

次のリストで、ログレコードのフィールドを順番に従い説明します。

#### timestamp

リクエストを受け取った時刻。この値は ISO-8601 の日時で、リクエストに対応したホストのシステムクロックに基づいています。

#### clientIp

リクエストを送信したクライアントの IP アドレス。

#### processingTime

MediaPackage でリクエストの処理に要した秒数。これは、リクエストの最終バイトが受信されてから、レスポンスの先頭バイトが送信されるまでの時間を計測した値です。

#### statusCode

レスポンスの HTTP ステータスの数値。

#### receivedBytes

MediaPackage サーバーが受信するリクエストボディのバイト数。

#### sentBytes

MediaPackage サーバーが送信するレスポンスボディのバイト数。この値は、多くの場合、サーバーレスポンスに含まれている Content-Length ヘッダーの値と同じです。

#### method

リクエストに使用された HTTP リクエストメソッド: DELETE、GET、HEAD、OPTIONS、PATCH、POST、または PUT。

## request

リクエスト URL。

## protocol

リクエストに使用されるプロトコルのタイプ (HTTP など)。

## userAgent

リクエスト送信元のクライアントを特定する user-agent 文字列 (二重引用符で囲まれます)。この文字列は、1 つ以上の製品 ID (製品/バージョン) で構成されます。文字列が 8 KB より長い場合は切り捨てられます。

## account

リクエストを行うために使用されたアカウントの AWS アカウント ID。

## channelId

リクエストを受信したチャンネルの ID。

## channelArn

リクエストを受信したチャンネルの Amazon リソースネーム (ARN)。

## domainName

TLS ハンドシェイク中にクライアントから提供される SNI (Server Name Indication) ドメイン (二重引用符で囲まれます)。クライアントで SNI をサポートしていない場合、あるいはドメインが証明書と一致せず、デフォルトの証明書がクライアントに提示された場合、この値は - となります。

## requestId

各リクエストを一意に識別するために MediaPackage で生成される文字列。

## endpointId

リクエストを受信したエンドポイントの ID。

## endpointArn

リクエストを受信したエンドポイントの Amazon リソースネーム (ARN)。

ログのフィールドの順序は変わることがあります。

## アクセスログを読み取る

MediaPackage は、Amazon CloudWatch Logs にアクセスログを書き込みます。CloudWatch Logs の一般料金が適用されます。アクセスログを読み取る際には、CloudWatch Logs のインサイトを利用します。CloudWatch Logs インサイトの使用方法の詳細については、AWS CloudWatch Logs ユーザーガイドの「[CloudWatch Logs Insights を使用したログデータの分析](#)」を参照してください。

### Note

CloudWatch にアクセスログが表示されるまでに数分かかることがあります。ログが表示されない場合は、数分後にもう一度お試しください。

### 例

このセクションでは、MediaPackage のデバッグログデータの読み取りに使用できるクエリ例を示しています。

Example チャンネルについての HTTP ステータスコードレスポンスを表示します。

このクエリを使用して、チャンネルの HTTP ステータスコード別のレスポンスを表示します。ここで表示される HTTP エラーコードレスポンスは、問題のトラブルシューティングに役立ちます。

```
fields @timestamp, @message
| filter channelId like 'my-channel'
| stats count() by statusCode
```

Example チャンネル上のエンドポイントあたりのリクエスト数を取得します。

```
fields @timestamp, @message
| filter channelId like 'my-channel'
| stats count() by endpointId
```

Example アセットごとのステータスコードを表示します。

```
fields @timestamp, @message
| filter assetArnlike 'my-asset-id'
| stats count() by statusCode
```



Example パッケージング設定の応答時間 (P99) を経時的に取得します。

```
fields @timestamp, @message
| filter packagingConfigArn like 'my-dash-config'
| stats pct(processingTime, 99) by bin(5m)
```

## マニフェストの更新時間のモニタリング

AWS Elemental MediaPackage 再生レスポンスには、非動的広告挿入ワークフローでマニフェストが MediaPackage 最後に変更された日時を示す次のカスタムヘッダーが含まれます。これらのヘッダーは、古いマニフェストに関連する問題のトラブルシューティングに役立ちます。

### XMediaPackage-マニフェスト-最後のシーケンス

これはマニフェストの最上位のセグメントシーケンス番号です。

- DASH では、これはマニフェストの最も低いレンディションの最上位のセグメント番号です。
- HLS および CMAF では、これはメディアプレイリストの最上位のセグメント番号です。
- MSS では、これはマニフェストの最上位のセグメント番号です。

[マニフェストの例](#)については、次のセクションを参照してください。

### XMediaPackage-Manifest-Last-Updated

が参照されるセグメント MediaPackage を生成するときのミリ秒単位のエポックタイムスタンプX-MediaPackage-Manifest-Last-Sequence。

## マニフェストの例

### DASH マニフェストの例

圧縮された DASH マニフェストと完全な DASH マニフェストの両方で、はマニフェストの最も低いレンディションで最も高いセグメント番号からX-MediaPackage-Manifest-Last-Sequence値 MediaPackage を決定します。このサービスでは、X-MediaPackage-Manifest-Last-Sequence で参照されるセグメントがいつ生成されるかに基づいて X-MediaPackage-Manifest-Last-Updated の値が計算されます。

## 継続時間を含む数値 - 圧縮マニフェスト

以下は、期間 template で番号を使用する圧縮 DASH マニフェストの例です。マニフェスト内の最も低いレンディションで最も高いセグメント番号から X-MediaPackage-Manifest-Last-Sequence 値 MediaPackage を決定します。例えば、次のマニフェストでは、最上位のセグメント番号が index\_video\_5\_0\_175232.mp4 であるため、X-MediaPackage-Manifest-Last-Sequence の値は 175232 です。がシーケンス\$Number\$値を計算する方法については MediaPackage、[SegmentTemplate での duration 属性](#)「」を参照してください。の値は、がで参照されるセグメント MediaPackage を生成するときのミリ秒単位の工ポックタイムスタンプX-MediaPackage-Manifest-Last-UpdatedですX-MediaPackage-Manifest-Last-Sequence。

```
<?xml version="1.0" encoding="utf-8"?>
<MPD xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns="urn:mpeg:dash:schema:mpd:2011"
  xsi:schemaLocation="urn:mpeg:dash:schema:mpd:2011 http://standards.iso.org/
  ittf/PubliclyAvailableStandards/MPEG-DASH_schema_files/DASH-MPD.xsd" id="201"
  type="dynamic" publishTime="2021-09-08T21:01:38" minimumUpdatePeriod="PT0S"
  availabilityStartTime="2018-11-16T19:08:30Z+00:00" minBufferTime="PT0S"
  suggestedPresentationDelay="PT0.000S" timeShiftBufferDepth="PT116.533S"
  profiles="urn:mpeg:dash:profile:isoff-live:2011">
  <Period start="PT0.000S" id="1">
    <AdaptationSet mimeType="video/mp4" segmentAlignment="true"
      subsegmentAlignment="true" startWithSAP="1" subsegmentStartsWithSAP="1"
      bitstreamSwitching="true">
      <SegmentTemplate timescale="30000" media="index_video_${RepresentationID}_${_}
      $Number$.mp4?m=1543947824" initialization="index_video_${RepresentationID}_${_}init.mp4?
      m=1543947824" startNumber="175032" duration="90000"/>
      <Representation id="1" width="640" height="360" frameRate="30/1"
        bandwidth="749952" codecs="avc1.640029"/>
      <Representation id="2" width="854" height="480" frameRate="30/1"
        bandwidth="1000000" codecs="avc1.640029"/>
      <Representation id="3" width="1280" height="720" frameRate="30/1"
        bandwidth="2499968" codecs="avc1.640029"/>
    </AdaptationSet>
  </Period>
</MPD>
```

## タイムライン付きの数値 - 圧縮マニフェスト

以下は、タイムライン template で番号を使用する圧縮 DASH マニフェストの例です。マニフェスト内の最も低いレンディションの最も高いセグメント番号から X-MediaPackage-Manifest-Last-

Sequence 値 MediaPackage を決定します。例えば、次のマニフェストでは、最上位のセグメント番号が `index_video_1_0_7.mp4` であるため、X-MediaPackage-Manifest-Last-Sequence の値は 7 です。この値は、`g` で参照されるセグメント MediaPackage を生成するときのミリ秒単位のエポックタイムスタンプ X-MediaPackage-Manifest-Last-Updated です X-MediaPackage-Manifest-Last-Sequence。

```
<?xml version="1.0" encoding="utf-8"?>
<MPD xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns="urn:mpeg:dash:schema:mpd:2011"
  xsi:schemaLocation="urn:mpeg:dash:schema:mpd:2011 http://standards.iso.org/
  ittf/PubliclyAvailableStandards/MPEG-DASH_schema_files/DASH-MPD.xsd" id="201"
  type="static" mediaPresentationDuration="PT72.458S" minBufferTime="PT0S"
  profiles="urn:mpeg:dash:profile:isoff-main:2011">
  <Period start="PT0.000S" id="1" duration="PT74.758S">
    <AdaptationSet mimeType="video/mp4" segmentAlignment="true" startWithSAP="1"
      subsegmentAlignment="true" subsegmentStartsWithSAP="1" bitstreamSwitching="true">
      <SegmentTemplate timescale="48000" media="index_video_${RepresentationID}_${_}
      $Number$.mp4?m=1621616401" initialization="index_video_${RepresentationID}_${_}init.mp4?
      m=1621616401" startNumber="1" presentationTimeOffset="108800">
        <SegmentTimeline>
          <S t="110400" d="540000" r="5"/>
          <S t="3350400" d="238000"/>
        </SegmentTimeline>
      </SegmentTemplate>
      <Representation id="1" width="640" height="480" frameRate="24/1"
        bandwidth="5000000" codecs="avc1.4D401E"/>
    </AdaptationSet>
    <AdaptationSet mimeType="audio/mp4" segmentAlignment="0" lang="eng">
      <Label>eng</Label>
      <SegmentTemplate timescale="48000" media="index_audio_${RepresentationID}_${_}
      $Number$.mp4?m=1621616401" initialization="index_audio_${RepresentationID}_${_}init.mp4?
      m=1621616401" startNumber="1" presentationTimeOffset="108800">
        <SegmentTimeline>
          <S t="108800" d="541696"/>
          <S t="650496" d="540672"/>
          <S t="1191168" d="539648" r="1"/>
          <S t="2270464" d="540672"/>
          <S t="2811136" d="539648"/>
          <S t="3350784" d="236544"/>
        </SegmentTimeline>
      </SegmentTemplate>
      <Representation id="2" bandwidth="192000" audioSamplingRate="48000"
        codecs="mp4a.40.2">
```

```

    <AudioChannelConfiguration
      schemeIdUri="urn:mpeg:dash:23003:3:audio_channel_configuration:2011" value="2"></
AudioChannelConfiguration>
    </Representation>
  </AdaptationSet>
  <SupplementalProperty schemeIdUri="urn:scte:dash:utc-time"
value="2021-05-21T16:59:47.450Z"></SupplementalProperty>
</Period>
</MPD>

```

## タイムライン付きの数値 - 圧縮マニフェスト

以下は、期間 template で番号を使用する圧縮 DASH マニフェストの例です。マニフェスト内の最も低いレンディションで最も高いセグメント番号から X-MediaPackage-Manifest-Last-Sequence 値 MediaPackage を決定します。例えば、次のマニフェストでは、最上位のセグメント番号が index\_video\_1\_0\_1675200.mp4 であるため、X-MediaPackage-Manifest-Last-Sequence の値は 1675200 です。がシーケンス番号を計算する方法については MediaPackage、[SegmentTemplate での media 属性](#)「」を参照してください。の値は、が参照されるセグメント MediaPackage を生成するときのミリ秒単位のエポックタイムスタンプ X-MediaPackage-Manifest-Last-Updated です X-MediaPackage-Manifest-Last-Sequence。

```

<?xml version="1.0" encoding="utf-8"?>
<MPD xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:mpeg:dash:schema:mpd:2011"
xsi:schemaLocation="urn:mpeg:dash:schema:mpd:2011 http://standards.iso.org/
ittf/PubliclyAvailableStandards/MPEG-DASH_schema_files/DASH-MPD.xsd" id="201"
type="static" mediaPresentationDuration="PT72.458S" minBufferTime="PT0S"
profiles="urn:mpeg:dash:profile:isoff-main:2011">
  <Period start="PT0.000S" id="1" duration="PT74.758S">
    <AdaptationSet mimeType="video/mp4" segmentAlignment="true" startWithSAP="1"
subsegmentAlignment="true" subsegmentStartsWithSAP="1" bitstreamSwitching="true">
      <SegmentTemplate timescale="48000" media="index_video_${RepresentationID}_${_}
${Time$.mp4?m=1621616401" initialization="index_video_${RepresentationID}_${_}init.mp4?
m=1621616401" startNumber="1" presentationTimeOffset="108800">
        <SegmentTimeline>
          <S t="55200" d="270000" r="5"/>
          <S t="1675200" d="119000"/>
        </SegmentTimeline>
      </SegmentTemplate>
      <Representation id="1" width="640" height="480" frameRate="24/1"
bandwidth="5000000" codecs="avc1.4D401E"/>
    </AdaptationSet>
  </Period>
</MPD>

```

```

</AdaptationSet>
<AdaptationSet mimeType="audio/mp4" segmentAlignment="0" lang="eng">
  <Label>eng</Label>
  <SegmentTemplate timescale="48000" media="index_audio_${RepresentationID$_0_
$Time$.mp4?m=1621616401" initialization="index_audio_${RepresentationID$_0_init.mp4?
m=1621616401" startNumber="1" presentationTimeOffset="108800">
    <SegmentTimeline>
      <S t="108800" d="541696"/>
      <S t="650496" d="540672"/>
      <S t="1191168" d="539648" r="1"/>
      <S t="2270464" d="540672"/>
      <S t="2811136" d="539648"/>
      <S t="3350784" d="236544"/>
    </SegmentTimeline>
  </SegmentTemplate>
  <Representation id="2" bandwidth="192000" audioSamplingRate="48000"
codecs="mp4a.40.2">
    <AudioChannelConfiguration
schemeIdUri="urn:mpeg:dash:23003:3:audio_channel_configuration:2011" value="2"></
AudioChannelConfiguration>
  </Representation>
</AdaptationSet>
<SupplementalProperty schemeIdUri="urn:scte:dash:utc-time"
value="2021-05-21T16:59:47.450Z"></SupplementalProperty>
</Period>
</MPD>

```

## HLS マニフェスト

MediaPackage は、マニフェストの最後のセグメント X-MediaPackage-Manifest-Last-Sequence の値を決定します。例えば次のマニフェストでは、index\_1\_3.ts が最上位のセグメントシーケンス番号であるため、X-MediaPackage-Manifest-Last-Sequence の値は 3 です。の値は、がマニフェスト内の最後のセグメント MediaPackage を生成するときの工ポックタイムスタンプをミリ秒単位で X-MediaPackage-Manifest-Last-Updated 表します。

```

#EXTM3U
#EXT-X-VERSION:3
#EXT-X-TARGETDURATION:8
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:7.500,
index_1_0.ts?m=1583172400
#EXTINF:7.500,
index_1_1.ts?m=1583172400

```

```
#EXTINF:7.500,  
index_1_2.ts?m=1583172400  
#EXTINF:7.500,  
index_1_3.ts?m=1583172400  
#EXT-X-ENDLIST
```

## CMAF マニフェスト

HLS と同様に、 はマニフェストの最後のセグメントX-MediaPackage-Manifest-Last-Sequenceの値 MediaPackage を決定します。例えば次のマニフェストでは、../cmfseg\_video\_1\_10.mp4?m=1621616399 が最上位のセグメントシーケンス番号であるため、X-MediaPackage-Manifest-Last-Sequence の値は 10 です。の値は、 がマニフェスト内の最後のセグメント MediaPackage を生成するときのエポックタイムスタンプをミリ秒単位でX-MediaPackage-Manifest-Last-Updated表します。

```
#EXTM3U  
#EXT-X-VERSION:6  
#EXT-X-INDEPENDENT-SEGMENTS  
#EXT-X-TARGETDURATION:12  
#EXT-X-MEDIA-SEQUENCE:1  
#EXT-X-MAP:URI="../cmfseg_video_1_track_1098178399_csid_aaa_2_init.mp4"  
#EXTINF:11.250,  
../cmfseg_video_1_1.mp4?m=1621616399  
#EXTINF:11.250,  
../cmfseg_video_1_2.mp4?m=1621616399  
#EXTINF:11.250,  
../cmfseg_video_1_3.mp4?m=1621616399  
#EXTINF:11.250,  
../cmfseg_video_1_4.mp4?m=1621616399  
#EXTINF:11.250,  
../cmfseg_video_1_5.mp4?m=1621616399  
#EXTINF:11.250,  
../cmfseg_video_1_6.mp4?m=1621616399  
#EXTINF:11.250,  
../cmfseg_video_1_7.mp4?m=1621616399  
#EXTINF:11.250,  
../cmfseg_video_1_8.mp4?m=1621616399  
#EXTINF:11.250,  
../cmfseg_video_1_9.mp4?m=1621616399  
#EXTINF:0.542,  
../cmfseg_video_1_10.mp4?m=1621616399  
#EXT-X-ENDLIST
```

## MSS マニフェスト

MediaPackage は、で示されているように、マニフェスト内の最も高いセグメントからX-MediaPackage-Manifest-Last-Sequence値を決定しますFragments(a\_2\_0={start time})。例えば次のマニフェストでは、Fragments(a\_2\_0=380533333) が最上位のシーケンス番号であるため、X-MediaPackage-Manifest-Last-Sequence の値は 380333333 です。の値は、がマニフェスト内の最後のセグメント MediaPackage を生成するときのエポックタイムスタンプをミリ秒単位でX-MediaPackage-Manifest-Last-Updated表します。

```
<SmoothStreamingMedia MajorVersion="2" MinorVersion="2" TimeScale="10000000"
CanSeek="TRUE" CanPause="TRUE" IsLive="TRUE" LookAheadFragmentCount="2"
DVRWindowLength="3000000000" Duration="0">
  <CustomAttributes>
    <Attribute Name="ProducerReferenceTime" Value="2017-06-14T22:07:01.967Z"/>
  </CustomAttributes>
  <StreamIndex Type="video" Name="video" Subtype="" Chunks="3" TimeScale="10000000"
Url="Events(203_0)/QualityLevels({bitrate})/Fragments(v={start time})"
QualityLevels="1">
    <QualityLevel Index="0" Bitrate="4000000"
CodecPrivateData="00000001274D401F924602802DD80880000003008000001E7220007A120000895477BDC07C22
FourCC="H264" MaxWidth="1280" MaxHeight="720"/>
    <c d="120000000" t="203333333"/>
    <c d="120000000"/>
    <c d="120000000"/>
  </StreamIndex>
  <StreamIndex Type="audio" Name="fra_1" Language="fra" Subtype=""
Chunks="3" TimeScale="10000000" Url="Events(203_0)/QualityLevels({bitrate})/
Fragments(a_2_0={start time})">
    <QualityLevel Index="0" Bitrate="128460" CodecPrivateData="1190" FourCC="AACL"
AudioTag="255" Channels="2" SamplingRate="48000" BitsPerSample="16" PacketSize="4"/>
    <c d="120533333" t="200000000"/>
    <c d="119893333"/>
    <c d="120106667"/>
  </StreamIndex>
</SmoothStreamingMedia>
```

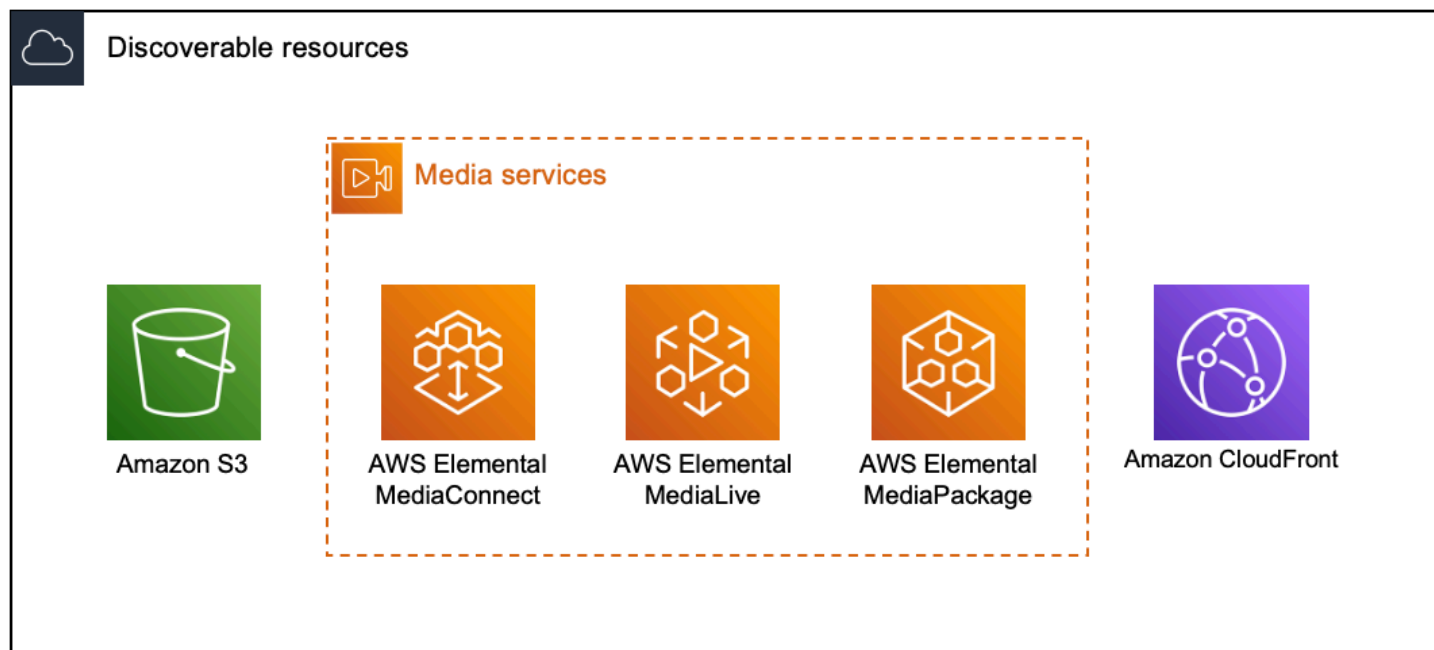


# ワークフローモニターを使用した AWS メディアサービスのモニタリング

ワークフローモニターは、AWS メディアワークフローの検出、可視化、モニタリングのためのツールです。ワークフローモニターは AWS、コンソールと API で使用できます。ワークフローモニターを使用して、シグナルマップと呼ばれるワークフローのリソースのビジュアルマッピングを検出して作成できます。Amazon CloudWatch アラーム EventBridge と Amazon ルールテンプレートを作成および管理して、マッピングされたリソースをモニタリングできます。作成したモニタリングテンプレートはデプロイ可能な AWS CloudFormation テンプレートに変換され、繰り返し性が確保されます。AWS が推奨するアラームテンプレートは、事前定義されたベストプラクティスのモニタリングを提供します。

## 検出


シグナルマップを使用して、メディアワークフローに関連付けられた相互接続された AWS リソースを自動的に検出します。検出は、サポートされている任意のサービスリソースから開始し、ワークフローの end-to-end マッピングを作成できます。シグナルマップは、スタンドアロンの視覚化ツールとして使用することも、モニタリングテンプレートで拡張することもできます。




## モニタリング

カスタム CloudWatch アラームと EventBridge ルールテンプレートを作成して、メディアワークフローのヘルスとステータスをモニタリングできます。ベストプラクティスのアラームテンプレート


は、ワークフローモニター環境にインポートできます。ベストプラクティスのアラームテンプレートはそのまま使用することも、ワークフローに合わせて編集することもできます。作成したテンプレートはすべて AWS CloudFormation テンプレートに変換され、繰り返しデプロイできます。




## Monitoring and deployment services




Amazon CloudWatch




Alarms




Logs




Amazon EventBridge



Rules



AWS CloudFormation



Stacks

### Note

ワークフローモニターの使用には直接コストはかかりません。ただし、ワークフローのモニタリングに作成および使用されるリソースにはコストがかかります。

モニタリングがデプロイされると、Amazon CloudWatch および Amazon EventBridge リソースが作成されます。AWS マネジメントコンソールを使用する場合、モニタリングをシグナルマップにデプロイする前に、作成されるリソースの数が通知されます。料金の詳細については、[CloudWatch「の料金」](#) および [EventBridge「の料金」](#) を参照してください。

ワークフローモニターは AWS CloudFormation テンプレートを使用して CloudWatch および EventBridge リソースをデプロイします。これらのテンプレートは、デプロイプロセス中にワークフローモニターによってユーザーに代わって作成される標準クラスの Amazon Simple Storage Service バケットに保存され、オブジェクトのストレージとリコールの料金が発生します。料金の詳細については、[Amazon S3の料金](#) を参照してください。

AWS Elemental MediaPackage チャンルのワークフローモニターシグナルマップで生成されたプレビューは MediaPackage、オリジンエンドポイントから配信され、データ転送出力料金が発生します。料金については、「[のMediaPackage料金](#)」を参照してください。

## ワークフロー 모니터のコンポーネント

ワークフローモニターには 4 つの主要コンポーネントがあります。

- CloudWatch アラームテンプレート - を使用してモニタリングする条件を定義します  
CloudWatch。独自のアラームテンプレートを作成するか、 によって作成された事前定義されたテンプレートをインポートできます AWS。詳細については、以下を参照してください。  
[CloudWatch アラームグループとテンプレート](#)
- EventBridge ルールテンプレート - アラームがトリガーされたときに が通知 EventBridge を送信する方法を定義します。詳細については、以下を参照してください。 [EventBridge ルールグループとテンプレート](#)
- シグナルマップ - 自動プロセスを使用して、既存の AWS リソースを使用して AWS Elemental ワークフローマップを作成します。シグナルマップを使用して、ワークフロー内のリソースを検出し、それらのリソースにモニタリングをデプロイできます。詳細については、以下を参照してください。 [ワークフローモニターのシグナルマップ](#)
- 概要 - 概要ページでは、1 つの場所から複数のシグナルマップのステータスを直接モニタリングできます。ワークフローのメトリクス、ログ、アラームを確認します。詳細については、以下を参照してください。 [ワークフローモニターの概要](#)

## サポートされる サービス

ワークフローモニターは、以下のサービスに関連するリソースの自動検出とシグナルマッピングをサポートしています。

- AWS Elemental MediaLive
- AWS Elemental MediaPackage
- AWS Elemental MediaConnect
- Amazon S3
- Amazon CloudFront

### トピック

- [ワークフローモニターの設定](#)
- [ワークフローモニターの使用](#)

## ワークフロー 모니터の設定

ワークフローモニターを初めてセットアップするには、アラームテンプレートとイベントテンプレートを作成し、メディアワークフローのモニタリングに使用されるシグナルマップを検出します。次のガイドには、管理者レベルとオペレーターレベルの IAM ロールの両方をセットアップし、ワークフローモニターリソースを作成し、モニタリングをワークフローにデプロイするために必要なステップが含まれています。

### トピック

- [ワークフローモニターの開始方法](#)
- [ワークフローモニターグループとテンプレート](#)
- [ワークフローモニターのシグナルマップ](#)
- [ワークフローモニターのクォータ](#)

### ワークフローモニターの開始方法

次の手順では、ワークフローモニターを初めて使用する際の基本的な概要を説明します。

1. セットアップワークフローは、管理者レベルとオペレーターレベルのロールの IAM アクセス許可をモニタリングします。 [ワークフローモニター IAM ポリシー](#)
2. アラームテンプレートを構築するか、 によって作成された事前定義されたテンプレートをインポートします AWS。 [CloudWatch アラーム](#)
3. によって配信される通知イベントを構築します EventBridge。 [EventBridge ルール](#)
4. 既存の AWS Elemental リソースを使用してシグナルマップを検出します。 [シグナルマップ](#)
5. アラームテンプレートと通知ルールをシグナルマップにアタッチします。 [テンプレートをアタッチする](#)
6. テンプレートをデプロイして、シグナルマップのモニタリングを開始します。 [モニタリングのデプロイ](#)
7. AWS コンソールの概要セクションを使用して、ワークフローモニターのリソースをモニタリングおよび確認します。 [概要](#)



## ワークフローモニター IAM ポリシー

ワークフローモニターは複数の AWS サービスとやり取りして、シグナルマップ、ビルド CloudWatch と EventBridge リソース、AWS CloudFormation テンプレートを作成します。ワークフローモニターはさまざまなサービスとやり取りするため、これらのサービスには特定の AWS Identity and Access Management (IAM) ポリシーを割り当てる必要があります。次の例は、管理者とオペレーターの両方の IAM ロールに必要な IAM ポリシーを示しています。

### 管理者 IAM ポリシー

次のポリシー例は、管理者レベルのワークフローモニター IAM ポリシー用です。このロールにより、ワークフローモニターリソースと、ワークフローモニターとやり取りするサポートされているサービスリソースの作成と管理が可能になります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:List*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:PutAnomalyDetector",
        "cloudwatch:PutMetricData",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutCompositeAlarm",
        "cloudwatch:PutDashboard",
        "cloudwatch>DeleteAlarms",
        "cloudwatch>DeleteAnomalyDetector",
        "cloudwatch>DeleteDashboards",
        "cloudwatch:TagResource",
        "cloudwatch:UntagResource"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:List*",
        "cloudformation:Describe*",
```

```
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation>DeleteStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "cloudfront:List*",
        "cloudfront:Get*"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeNetworkInterfaces"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "events:List*",
        "events:Describe*",
        "events:CreateEventBus",
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
        "events>DeleteRule",
        "events:RemoveTargets",
        "events:TagResource",
        "events:UntagResource"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "logs:Describe*",
```

```
    "logs:Get*",
    "logs:TagLogGroup",
    "logs:TagResource",
    "logs:UntagLogGroup",
    "logs:UntagResource"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "mediaconnect:List*",
    "mediaconnect:Describe*"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "medialive:*"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "mediapackage:List*",
    "mediapackage:Describe*"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "mediapackagev2:List*",
    "mediapackagev2:Get*"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "mediapackage-vod:List*",
    "mediapackage-vod:Describe*"
  ]
}
```



```
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "mediatailor:List*",
      "mediatailor:Describe*",
      "mediatailor:Get*"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "resource-groups:ListGroup",
      "resource-groups:GetGroup",
      "resource-groups:GetTags",
      "resource-groups:GetGroupQuery",
      "resource-groups:GetGroupConfiguration",
      "resource-groups:CreateGroup",
      "resource-groups:UngroupResources",
      "resource-groups:GroupResources",
      "resource-groups>DeleteGroup",
      "resource-groups:UpdateGroupQuery",
      "resource-groups:UpdateGroup",
      "resource-groups:Tag",
      "resource-groups:Untag"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:*"
    ],
    "Resource": "arn:aws:s3:::workflow-monitor-templates*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "sns:TagResource",
      "sns:UntagResource"
    ],
  },
```

```
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "tag:Get*",
      "tag:Describe*",
      "tag:TagResources",
      "tag:UntagResources"
    ],
    "Resource": "*"
  }
]
```

## オペレーター IAM ポリシー

次のポリシー例は、オペレータレベルのワークフローモニター IAM ポリシー用です。このロールは、ワークフローモニターリソースと、ワークフローモニターとやり取りするサポートされているサービスリソースへの制限付き読み取り専用アクセスを許可します。

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

```

```
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "cloudfront:List*",
      "cloudfront:Get*"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeNetworkInterfaces"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "events:List*",
      "events:Describe*"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "logs:Describe*",
      "logs:Get*"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "mediaconnect:List*",
      "mediaconnect:Describe*"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
```

```
    "medialive:List*",
    "medialive:Get*",
    "medialive:Describe*"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "mediapackage:List*",
    "mediapackage:Describe*"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "mediapackagev2:List*",
    "mediapackagev2:Get*"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "mediapackage-vod:List*",
    "mediapackage-vod:Describe*"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "mediatailor:List*",
    "mediatailor:Describe*",
    "mediatailor:Get*"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "s3:Get*",
    "s3:List*"
  ]
}
```

```
    ],
    "Resource": "arn:aws:s3:::workflow-monitor-templates*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "tag:Get*",
      "tag:Describe*"
    ],
    "Resource": "*"
  }
]
```

## ワークフローモニターグループとテンプレート

ワークフローモニタリングをシグナルマップにデプロイする前に、CloudWatch アラームと EventBridge 通知のグループとテンプレートを作成する必要があります。CloudWatch テンプレートは、アラームのトリガーに使用するシナリオとしきい値を定義します。EventBridge テンプレートによって、これらのアラームがどのように報告されるかが決まります。

接続されたリソースのマッピングのみが必要で、ワークフローモニターのモニタリングテンプレート機能を使用しない場合は、CloudWatch および EventBridge テンプレートなしでシグナルマップを使用できます。シグナルマップの使用の詳細については、以下を参照してください。 [シグナルマップ](#)

### トピック

- [CloudWatch アラームグループとテンプレート](#)
- [EventBridge ルールグループとテンプレート](#)

## CloudWatch アラームグループとテンプレート

ワークフローモニターアラームを使用すると、シグナルマップのアラームの基盤として既存の CloudWatch メトリクスを使用できます。アラームテンプレートグループを作成して、ワークフローにとって重要なアラームのタイプをソートおよび分類できます。各アラームテンプレートグループ内で、モニタリングする特定の CloudWatch メトリクスとパラメータを含むアラームテンプレートを作成します。独自のアラームテンプレートを作成するか、によって作成された推奨アラームテンプレートをインポートできます AWS。そのグループ内にアラームテンプレートグループとアラームテ

ンプレートを作成したら、これらのアラームテンプレートグループの1つ以上をシグナルマップにアタッチできます。

最初にアラームテンプレートグループを作成する必要があります。アラームテンプレートグループを作成したら、独自のテンプレートを作成するか、によって作成された推奨テンプレートを使用できます AWS。独自のアラームテンプレートを作成する場合は、このページに進みます。推奨テンプレートのインポートの詳細については、以下を参照してください。 [推奨テンプレート](#)

このセクションでは、ワークフローモニターを使用した CloudWatch アラームの作成について説明します。CloudWatch サービスによるアラームの処理方法とアラームコンポーネントの詳細については、「Amazon CloudWatch [ユーザーガイド](#)」の [CloudWatch](#) 「アラームの使用」を参照してください。

## アラームテンプレートグループの作成

アラームテンプレートグループを作成するには

1. ワークフローモニターコンソールのナビゲーションペインから、CloudWatchアラームテンプレート を選択します。
2. アラームテンプレートグループの作成 を選択します。
3. アラームテンプレートグループに一意のグループ名とオプションの説明 を付けます。
4. 作成 を選択すると、新しく作成されたアラームテンプレートグループの詳細ページが表示されます。

## アラームテンプレートの作成

アラームテンプレートを作成するには

1. アラームテンプレートグループの詳細ページから、アラームテンプレートの作成 を選択します。
2. アラームテンプレートに一意のテンプレート名とオプションの説明 を付けます。
3. 「メトリクスの選択」セクションで、次の操作を行います。
  1. ターゲットリソースタイプ を選択します。ターゲットリソースタイプは、 のチャンネル MediaLive や の MediaPackage フローなど、それぞれのサービスのリソースです MediaConnect。
  2. メトリクス名 を選択します。これは、 CloudWatchアラームの基盤となるメトリクスです。メトリクスのリストは、選択したターゲットリソースタイプ に応じて変わります。

#### 4. アラーム設定 セクションで、次の操作を行います。

##### Note

CloudWatch サービスがアラームを処理する方法とアラームコンポーネントの詳細については、「Amazon CloudWatch [ユーザーガイド](#)」の [CloudWatch](#) 「アラームの使用」を参照してください。

1. **統計** を選択します。これは、メトリクスのモニタリングに使用される合計や平均などの値です。
  2. **比較演算子** を選択します。このフィールドは、次のステップで設定したしきい値を参照します。
  3. **しきい値** を設定します。これは、比較演算子がステータスより大きい、小さい、または等しいかどうかを判断するために使用される数値です。
  4. **期間** を設定します。これは秒単位の時間値です。Period は、統計、比較演算子、しきい値が相互作用してアラームがトリガーされるかどうかを判断する時間の長さです。
  5. **データポイント** を設定します。この値は、アラームをトリガーするために必要なデータポイントの数を決定します。
  6. **欠落データの処理方法** を選択します。この選択により、このアラームが欠落データにどのように反応するかが決まります。
5. **作成** を選択してプロセスを完了します。

完了したアラームテンプレートの例には、次のパラメータを含めることができます。MediaConnect フローターゲットリソースタイプは、切断メトリクス名 についてモニタリングされます。統計値は Sum に設定され、比較演算子は「より大きい」、しきい値は 10 です。期間は 60 秒に設定され、必要なデータポイントは 1 つのうち 1 つのみです。欠落データの処理は「無視」に設定されています。

これらの設定の結果、ワークフローモニターはフローの切断をモニタリングします。60 秒以内に 10 回以上の切断が発生すると、アラームがトリガーされます。60 秒以内に 10 回以上の切断を行うだけで、アラームがトリガーされます。

#### 推奨されるアラームテンプレート

ワークフローモニターの推奨テンプレートは、メトリクスに適した事前定義されたアラーム設定を持つ AWS Elemental サービスメトリクスの厳選された選択です。カスタマイズされたアラームテンプレート

レートを作成しない場合は、が作成したベストプラクティスのモニタリングテンプレートが推奨テンプレートに用意されています AWS。

ワークフローモニターには、サポートされている各サービスに推奨されるテンプレートグループが含まれています。これらのグループは、特定のタイプのワークフローにベストプラクティスのモニタリングを適用するように設計されています。各テンプレートグループには、サービス固有のメトリクスから設定されたアラームの厳選された選択が含まれています。例えば、MediaLive マルチプレックスワークフローに推奨されるテンプレートグループには、MediaConnect CDI ワークフローとは異なる事前設定されたメトリクスのセットがあります。

推奨アラームテンプレートを使用するには

1. 手順に従って[アラームテンプレートグループを作成する](#)か、既存のテンプレートグループを選択します。
2. アラームテンプレートセクションで、のインポートを選択します。AWS 推奨テンプレートをテンプレートグループにインポートする必要があります。
3. CloudWatch アラームテンプレートグループのドロップダウンを使用して、AWS 推奨グループを選択します。これらのグループには、特定の サービス用に厳選されたアラームが含まれています。
4. チェックボックスを使用して、インポートするテンプレートを選択します。各テンプレートには、メトリクス、事前設定されたモニタリング値、メトリクスの説明が一覧表示されます。テンプレートの選択が完了したら、追加 ボタンを選択します。
5. 選択したテンプレートは、アラームテンプレート (複数可) に移動してインポートセクションに移動します。選択内容を確認し、インポート を選択します。
6. インポートが完了すると、選択したテンプレートがテンプレートグループに追加されます。さらにテンプレートを追加する場合は、インポートプロセスを繰り返します。
7. インポートされたテンプレートは、インポート後にカスタマイズできます。アラーム設定は、アラームのニーズに合わせて変更できます。

## EventBridge ルールグループとテンプレート

CloudWatch は Amazon EventBridge ルールを使用して通知を送信します。作成したイベントテンプレートに基づいて通知を送信できます。まず、イベントテンプレートグループを作成します。そのイベントテンプレートグループでは、通知を作成する条件と通知を受け取るユーザーを決定するイベントテンプレートを作成します。



このセクションでは、ワークフローモニターを使用した EventBridge ルールの作成について説明します。EventBridge サービスがルールを使用する方法の詳細については、「Amazon ユーザーガイド」の「[EventBridge ルール](#)」を参照してください。EventBridge

## イベントテンプレートグループの作成

イベントテンプレートグループを作成するには

1. ワークフローモニターコンソールのナビゲーションペインから、EventBridge ルールテンプレートを選択します。
2. イベントテンプレートグループの作成 を選択します。
3. アラームテンプレートグループに一意のグループ名とオプションの説明 を付けます。
4. 作成 を選択すると、新しく作成されたアラームテンプレートグループの詳細ページが表示されます。

## イベントテンプレートの作成

イベントテンプレートを作成するには

1. イベントテンプレートグループの詳細ページから、イベントテンプレートの作成 を選択します。
2. イベントテンプレートに一意のテンプレート名とオプションの説明 を付けます。
3. ルール設定 セクションで：
  1. イベントタイプ を選択します。イベントタイプを選択するときは、 によって作成された複数のイベントから選択 AWS するか、シグナルマップアクティブアラームを選択して、アラームテンプレートによって作成されたアラームを使用できます。
  2. ターゲットサービス を選択します。これにより、このイベントをどのように通知するかが決まります。Amazon Simple Notification Service または CloudWatch ログを選択できます。
  3. ターゲットサービスを選択したら、ターゲット を選択します。これは、ターゲットサービスの選択に応じて、Amazon SNS トピックまたは CloudWatch ロググループになります。
4. 作成を選択してプロセスを完了します。

## ワークフローモニターのシグナルマップ

シグナルマップは、メディアワークフロー内の AWS リソースの視覚的なマッピングです。ワークフローモニターを使用して、サポートされている任意のリソースタイプでシグナルマップ検出を開始で

きます。検出プロセス中、ワークフローモニターは接続されているすべての AWS リソースを自動的に再帰的にマッピングします。シグナルマップを作成したら、ワークフローモニターコンソールを使用して、モニタリングテンプレートのデプロイ、メトリクスの表示、マッピングされたリソースの詳細の表示などを行うことができます。

## トピック

- [シグナルマップの作成](#)
- [シグナルマップの表示](#)
- [アラームテンプレートとイベントテンプレートをシグナルマップにアタッチする](#)
- [シグナルマップへのテンプレートのデプロイ](#)
- [シグナルマップと基盤となるリソースの更新](#)
- [シグナルマップの削除](#)

## シグナルマップの作成

シグナルマップを作成するには

1. ワークフローモニターコンソールのナビゲーションペインから、シグナルマップ を選択します。
2. シグナルマップの作成 を選択します。
3. シグナルマップに名前 と説明 を付けます。
4. 「新しいシグナルマップの検出」セクションに、現在のアカウントと選択したリージョンのリソースが表示されます。シグナルマップの検出を開始するリソースを選択します。選択したリソースが検出の開始点になります。
5. [作成] を選択します。検出プロセスが完了するまでしばらくお待ちください。プロセスが完了すると、新しいシグナルマップが表示されます。

### Note

AWS Elemental MediaPackage チャンネルのワークフローモニターシグナルマップで生成されたプレビューは MediaPackage 、オリジンエンドポイントから配信され、データ転送出力料金が発生します。料金については、「[のMediaPackage料金](#)」を参照してください。

## シグナルマップの表示

### シグナルマップビュー

シグナルマップを選択すると、シグナルマップのモニタリングまたは設定に使用できる 2 つのビューが表示されます。Monitor シグナルマップと Configure シグナルマップは、シグナルマップコンソールセクションの右上にあるコンテキスト依存ボタンです。

ナビゲーションペインの「シグナルマップ」セクションを使用してシグナルマップを選択すると、シグナルマップが設定ビューに表示されます。設定ビューでは、このシグナルマップにアタッチされたテンプレートグループを変更したり、アタッチされたテンプレートをデプロイしたり、シグナルマップの基本的な詳細とタグを表示したりできます。

ナビゲーションペインの概要セクションを使用してシグナルマップを選択すると、シグナルマップがモニタリングビューに表示されます。モニタリングビューには、このシグナルマップの CloudWatch アラーム、EventBridge ルール、アラート、ログ、メトリクスが表示されます。

右上のシグナルマップのモニタリング/設定ボタンを選択すると、いつでもビューを変更できます。設定ビューには、管理者レベルの IAM アクセス許可が必要です。必要な IAM アクセス許可は、こちらで確認できます。 [ワークフローモニター IAM ポリシー](#)

### シグナルマップのナビゲーション

シグナルマップには、ワークフローモニターによって検出されたサポートされているすべての AWS リソースのノードが含まれます。サムネイルプレビューが利用可能な場合、MediaLive チャンネルや MediaPackage エンドポイントなどの特定のリソースにコンテンツのサムネイルプレビューを表示できます。

リソースノードを選択し、アクションドロップダウンメニューから選択したリソースの詳細を表示するを選択すると、関連するサービスの詳細ページが表示されます。例えば、MediaLive チャンネルを選択し、選択したリソースの詳細を表示を選択すると、そのチャンネルの MediaLive コンソールの詳細ページが開きます。

リソースノードを選択すると、アクティブなアラームのリストがそのノードのみにフィルタリングされます。アクティブなアラームでリソースのターゲット ARN を選択すると、関連付けられたサービスの詳細ページが表示され、選択したリソースが開かれます。

### アラームテンプレートとイベントテンプレートをシグナルマップにアタッチする

アラームテンプレートとイベントテンプレートを作成したら、それらをシグナルマップにアタッチする必要があります。作成したアラームテンプレートとイベントテンプレートは、検出されたシグナルマップにアタッチできます。

## アラームテンプレートとイベントテンプレートをシグナルマップにアタッチするには

1. ワークフローモニターコンソールのナビゲーションペインから、シグナルマップを選択し、操作するシグナルマップを選択します。
2. シグナルマップページの右上にあるCloudWatchアラームテンプレートグループタブで、CloudWatch アラームテンプレートグループをアタッチを選択します。
  1. 開いた新しいセクションで、このシグナルマップに適用するすべてのアラームテンプレートグループを選択し、の追加を選択します。これにより、選択したアラームテンプレートグループが「アタッチされたアラームテンプレートグループ CloudWatch」セクションに移動します。
  2. 保存を選択すると、変更が保存され、シグナルマップページに戻ります。
3. シグナルマップページの右側で、EventBridge ルールテンプレートグループタブを選択し、ルールテンプレートグループ EventBridgeのアタッチを選択します。
  1. 開いた新しいセクションで、このシグナルマップに適用するすべてのイベントテンプレートグループを選択し、の追加を選択します。これにより、選択したルールテンプレートグループがアタッチされた EventBridge ルールテンプレートグループセクションに移動します。
  2. 保存を選択すると、変更が保存され、シグナルマップページに戻ります。
4. CloudWatch アラームテンプレートと EventBridge ルールテンプレートをシグナルマップに割り当てましたが、モニタリングはまだデプロイされていません。次のセクションでは、モニタリングリソースのデプロイについて説明します。

## シグナルマップへのテンプレートのデプロイ

アラームテンプレートとイベントテンプレートをシグナルマップにアタッチしたら、モニタリングをデプロイする必要があります。デプロイが完了するまで、シグナルマップのモニタリングはアクティブになりません。

ワークフローモニターは、選択したシグナルマップに関連するアラームのみをデプロイします。例えば、アタッチされたアラームテンプレートグループには、MediaLive MediaPackage、などの複数のサービスのアラームが含まれている場合があります MediaConnect。選択したシグナルマップにリソースのみが含まれている場合 MediaLive、MediaPackage または MediaConnect アラームはデプロイされません。

## モニタリングテンプレートをデプロイするには

1. アラームおよびイベントテンプレートグループをシグナルマップにアタッチし、変更を保存したら、アクションドロップダウンメニューでモニターをデプロイを選択します。
2. デプロイを確認するように求められ、作成される CloudWatch と EventBridge リソースの数が表示されます。続行する場合は、デプロイを選択します。

### Note

ワークフローモニターの使用には直接コストはかかりません。ただし、ワークフローのモニタリングに作成および使用されるリソースにはコストがかかります。

モニタリングがデプロイされると、Amazon リソース CloudWatch と Amazon EventBridge リソースが作成されます。AWS マネジメントコンソールを使用する場合、モニタリングをシグナルマップにデプロイする前に、作成されるリソースの数が通知されます。料金の詳細については、[CloudWatch「の料金」](#)および[EventBridge「の料金」](#)を参照してください。

ワークフローモニターは AWS CloudFormation テンプレートを使用して CloudWatch および EventBridge リソースをデプロイします。これらのテンプレートは、デプロイプロセス中にワークフローモニターによってユーザーに代わって作成される標準クラスの Amazon Simple Storage Service バケットに保存され、オブジェクトのストレージとリコールの料金が発生します。料金の詳細については、[Amazon S3の料金](#)を参照してください。

3. デプロイのステータスは、シグナルマップの名前の横に表示されます。デプロイステータスは、AWS CloudFormation コンソールの スタック セクションにも表示されます。リソースの作成とデプロイがしばらく続くと、シグナルマップのモニタリングが開始されます。

## シグナルマップと基盤となるリソースの更新

ワークフローに変更があった場合は、シグナルマップを再検出し、モニタリングリソースを再デプロイする必要がある場合があります。ワークフローモニターは、ワークフローに変更を加える機能を持たない視覚化およびモニタリングツールです。シグナルマップはワークフローの point-in-time 視覚化を表します。メディアワークフローの一部を追加、削除、または大幅に変更する場合は、シグナルマップを再検出することをお勧めします。シグナルマップにモニタリングリソースがアタッチされている場合は、再検出プロセスの後にモニタリングを再デプロイすることをお勧めします。

## シグナルマップを再検出するには

1. ワークフローモニターコンソールのナビゲーションペインから、シグナルマップを選択し、操作するシグナルマップを選択します。
2. シグナルマップの設定ビューが表示されていることを確認します。ビューの変更の詳細については、以下を参照してください。 [シグナルマップを表示する](#)
3. シグナルマップページの右上で、アクションドロップダウンメニューを選択します。再検出 を選択します。
4. 再検出画面が表示されます。再検出するワークフローの一部であるリソースを選択します。再検出ボタンを選択します。
5. シグナルマップは、現在のワークフローに従って再構築されます。モニタリングリソースを再デプロイする必要がある場合は、このシグナルマップのページにとどまります。以前にアタッチされたモニタリングテンプレートはアタッチされたままになりますが、再デプロイする必要があります。

## シグナルマップの再検出後にモニタリングテンプレートを再デプロイするには

1. 再検出後、更新されたシグナルマップに移動します。モニタリングテンプレートを再デプロイするには、アクションドロップダウンメニューからモニターをデプロイを選択します。
2. デプロイを確認するように求められ、作成されるすべての CloudWatch および EventBridge リソースの数が表示されます。続行する場合は、デプロイ を選択します。
3. デプロイのステータスは、シグナルマップの名前の横に表示されます。リソースの作成とデプロイがしばらく続くと、シグナルマップのモニタリングが開始されます。

## シグナルマップの削除

シグナルマップが不要になった場合は、削除できます。シグナルマップにモニタリングテンプレートをデプロイしている場合、削除プロセスにより、このシグナルマップにデプロイされた CloudWatch および EventBridge リソースをすべて削除するよう求められます。デプロイされたリソースを削除しても、それらを作成したテンプレートには影響しません。このリソースの削除は、デプロイされているが使用されていない CloudWatch および EventBridge リソースがないことを確認するためです。

## シグナルマップを削除するには

1. ワークフローモニターコンソールのナビゲーションペインで、シグナルマップを選択し、削除するシグナルマップの横にあるラジオボタンを選択します。

2. [削除] ボタンを選択します。モニタリングリソースの削除を確認するよう求められます。削除を選択して、モニタリングリソースの削除プロセスを開始します。
3. Monitor デプロイ列に現在のステータスが表示されます。ステータスが DELETE\_COMPLETE に変わったら、削除ボタンを再度選択します。
4. シグナルマップの削除を確認するよう求められます。削除を選択して続行し、シグナルマップを削除します。

## ワークフローモニターのクォータ

次のセクションには、ワークフローモニターリソースのクォータが含まれています。各クォータは「アカウントごと」ベースです。1つのAWSアカウントで次のクォータを超えることはできません。これらのクォータを増やすことはできません。

### クォータ

リソースタイプ	クォータ
CloudWatch アラームテンプレートグループ	20
CloudWatch アラームテンプレート	200
EventBridge ルールテンプレートグループ	20
EventBridge ルールテンプレート	200
シグナルマップ	30
シグナルマップ: 1つのシグナルマップ内のリソースノード	30
1つのシグナルマップにアタッチされたシグナルマップ : CloudWatch アラームテンプレートグループ	5
シグナルマップ: 1つのシグナルマップにアタッチされた EventBridge ルールテンプレートグループ	5



## ワークフローモニターの使用

ワークフローモニターコンソールの概要とシグナルマップセクションを使用して、ワークフローの現在のステータス、および関連するアラーム、メトリクス、ログを確認します。

### トピック

- [ワークフローモニターの概要](#)
- [概要ログとメトリクス](#)
- [ワークフローモニターのシグナルマップの使用](#)

## ワークフローモニターの概要

ワークフローモニターコンソールの概要セクションは、シグナルマップ at-a-glance に関する情報を提供するダッシュボードです。概要セクションでは、各シグナルマップのモニタリングの現在の状態と、CloudWatch メトリクスおよび関連する CloudWatch ログを確認できます。そのシグナルマップコンソールページに移動するシグナルマップを選択できます。

### 概要フィルタリング

概要セクションの検索バーを使用すると、コンテキスト機密制約を使用してシグナルマップのリストをフィルタリングできます。検索バーを選択すると、フィルタリングするプロパティのリストが表示されます。プロパティを選択すると、等号、包含、不等号、不等号などの演算子が表示されます。演算子を選択すると、選択したプロパティタイプからリソースのリストが作成されます。これらのリソースのいずれかを選択すると、シグナルマップリストには、定義した制約に適合するシグナルマップのみが表示されます。

## 概要ログとメトリクス

シグナルマップの CloudWatch メトリクスとログを表示するには、シグナルマップの名前の横にあるラジオボタンを選択します。メトリクスとログの両方のタブ付きインターフェイスがシグナルマップリストの下に表示されます。

### CloudWatch メトリクス

CloudWatch 選択したシグナルマップのメトリクスはコンテキスト依存であり、そのシグナルマップワークフローで使用されるサービスに関連付けられたメトリクスのみを表示します。画面上のメトリクスツールを使用して、表示されるメトリクスの期間と時間範囲をカスタマイズできます。

### CloudWatch ログ



CloudWatch ロググループをシグナルマップに関連付けた場合、そのグループがここに表示されません。

## ワークフロー 모니터のシグナルマップの使用

コンソールの概要セクションから特定のシグナルマップを選択すると、そのシグナルマップとそのアタッチされたモニタリングリソースに関する詳細情報を表示できます。

シグナルマップを選択すると、シグナルマップと、詳細情報を含むタブ付きセクションがいくつか表示されます。

- CloudWatch アラーム
- EventBridge ルール
- AWS Elemental アラート
- メトリクス
- ログ
- 基本的な詳細

## シグナルマップのナビゲーション

シグナルマップには、ワークフローモニターによって検出されたサポートされているすべての AWS リソースのノードが含まれます。サムネイルプレビューが利用可能な場合、MediaLive チャネルや MediaPackage エンドポイントなどの特定のリソースにコンテンツのサムネイルプレビューを表示できます。

リソースノードを選択し、アクションドロップダウンメニューから選択したリソースの詳細を表示するを選択すると、関連するサービスの詳細ページが表示されます。例えば、MediaLive チャネルを選択し、選択したリソースの詳細を表示を選択すると、そのチャネルの MediaLive コンソールの詳細ページが開きます。

リソースノードを選択すると、アクティブなアラームのリストがそのノードのみにフィルタリングされます。アクティブなアラームでリソースのターゲット ARN を選択すると、関連付けられたサービスの詳細ページが表示され、選択したリソースが開かれます。

# AWS Elemental MediaPackage リソースのタグ付け

タグとは、AWS リソースに割り当てるラベルです。タグはそれぞれ、1つのキーと1つの値で構成されており、どちらもお客様側が定義します。例えば、タグキーは「stage」、タグ値は「test」などです。タグは、さまざまな目的で使用できます。一般的な用途の1つは、タグを使用してAWS リソースへのアクセスを管理することです。詳細については、IAM ユーザーガイドの「[タグを使用したAWS リソースへのアクセスの制御](#)」を参照してください。

もう1つのタグの一般的な用途は、MediaPackage のコストの分類と追跡です。コスト配分タグをMediaPackage のチャンネル、エンドポイント、パッケージング設定に適用すると、AWS では、コスト配分レポートがコンマ区切り値 (CSV) ファイルとして生成され、使用量とコストがタグごとに集計されます。自社のカテゴリ (たとえばコストセンター、アプリケーション名、所有者) を表すタグを適用すると、複数のサービスにわたってコストを分類することができます。タグを使ったコスト配分の詳細については、[AWS Billing ユーザーガイドのコスト配分タグの使用](#)を参照してください。

## タグの制限

AWS Elemental MediaPackage リソースのタグ付けには以下のような制限があります。

- コスト配分のタグ付けは、チャンネル、エンドポイント、およびパッケージング設定のリソースでのみ使用できます。アセットまたはパッケージグループのリソースにコスト配分タグを使用することはできません。
- リソースに割り当てることができるタグの最大数: 50
- キーの最大長 — 128 文字 (Unicode)
- 値の最大長 — 256 文字 (Unicode)
- キーと値で有効な文字 — a~z、A~Z、0~9、スペース、および特殊文字 ( \_ . : / = + - @ )
- キーと値は大文字と小文字が区別されます。
- aws: をキーのプレフィックスとしてを使用しないでください。AWS 用に予約済みです。
- 収集した Live-to-VOD アセットには使用できません。

## タグの管理

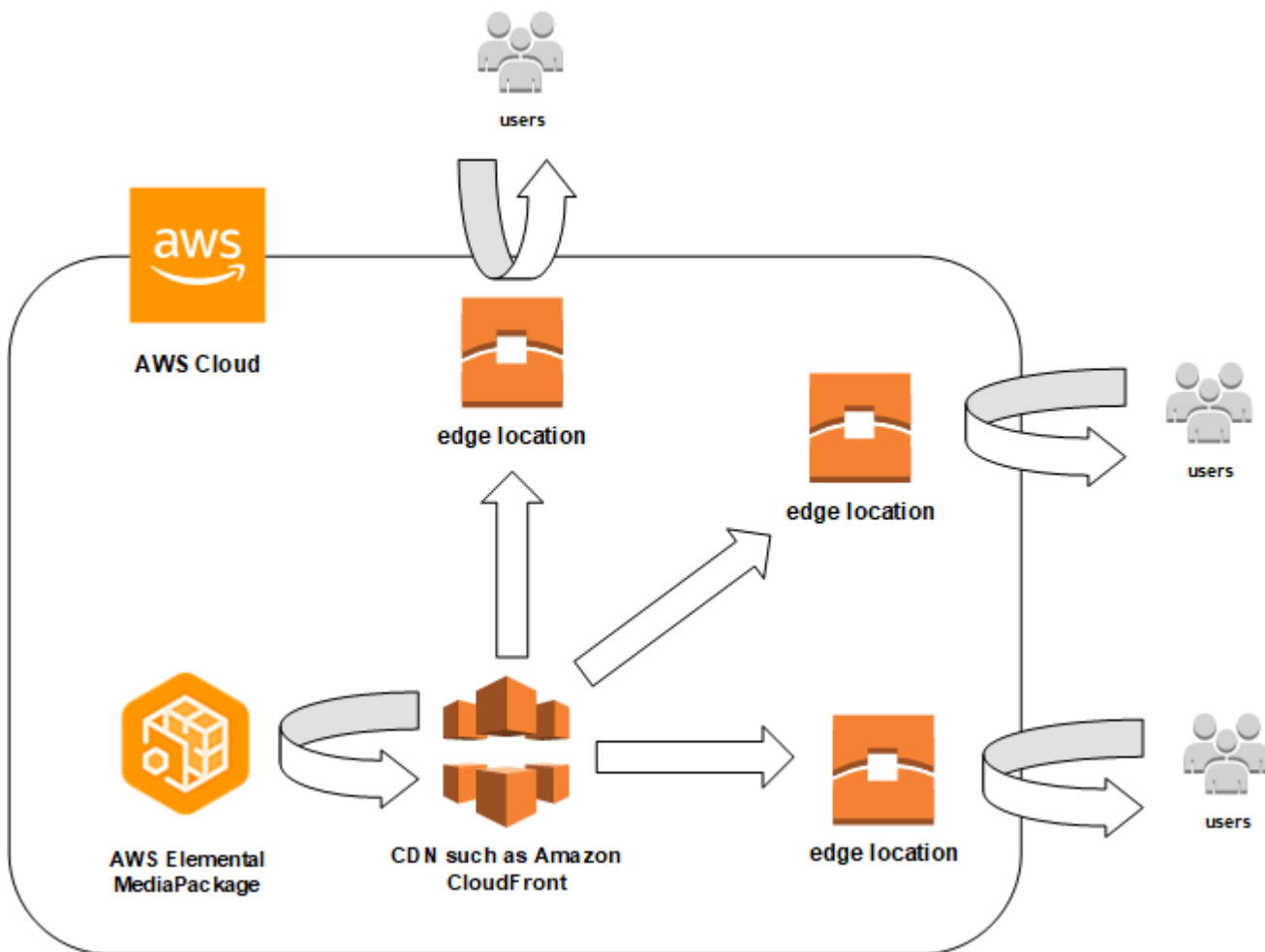
AWS Elemental MediaPackage API または AWS CLI を使用して、これらのプロパティの値を追加、編集、または削除できます。

詳細については、次の参照ドキュメントのタグに関連するアクションを参照してください。

- AWS Elemental MediaPackage ライブ API リファレンスの「[Tags resource-arn](#)」
- AWS Elemental MediaPackage VOD API リファレンスの「[Tags resource-arn](#)」
- AWS CLI MediaPackage リファレンスの「[tag-resource](#)」

## CDN の使用

[Amazon CloudFront](#) などのコンテンツ配信ネットワーク (CDN) を使用して、に保存したコンテンツを配信できますAWS Elemental MediaPackage。CDN は、グローバルに分散されたサーバーのセットであり、動画などのコンテンツをキャッシュします。ユーザーがコンテンツをリクエストすると、CDN はそのリクエストを最もレイテンシーが低いエッジロケーションにルーティングします。コンテンツがこのエッジロケーションにキャッシュ済みである場合、CDN はコンテンツを直ちに配信します。コンテンツがこのエッジロケーションに現在存在しない場合、CDN はオリジン (この場合は MediaPackage エンドポイント) からコンテンツを取得し、ユーザーに配信します。次の図はこのプロセスを示しています。



以下のセクションでは、Amazon のディストリビューションを操作する手順について説明します CloudFront。

### トピック

- [ディストリビューションの作成](#)

- [ディストリビューションを表示する](#)
- [ディストリビューションを編集する](#)
- [ディストリビューションを削除する](#)

## ディストリビューションの作成

Amazon のディストリビューションは、コンテンツの配信元や追跡および管理方法など、コンテンツ配信に関するすべての情報 CloudFront を保持します。ディストリビューションで保持される情報には、オリジン (コンテンツの配信元) と動作 (コンテンツのリクエストをルーティングするためにリクエストで指定されたパターン) があります。

ディストリビューションは、CloudFrontコンソールから作成できます。次のセクションでは、このアプローチについて説明します。

### トピック

- [Amazon からのディストリビューションの作成 CloudFront](#)

## Amazon からのディストリビューションの作成 CloudFront

AWS Elemental MediaPackage にチャンネルとそのエンドポイントを作成したら、各エンドポイントの URL を書き留めます。これらの URLs は、CloudFront ディストリビューションのオリジンドメイン名に使用します。MediaPackage のチャンネルのエンドポイントごとにオリジンが 1 つ必要です。

CloudFront AWS Elemental MediaPackage エンドポイントオリジンとするディストリビューションを Amazon で作成する詳細な手順については、Amazon CloudFront [デベロッパーガイドの「ライブストリーミングビデオの配信」](#) を参照してください。

## ディストリビューションを表示する

「[チャンネルの詳細の表示](#)」で説明しているように、ディストリビューション ID や概要など、MediaPackage で作成したディストリビューションに関する基本的な情報を表示できます。ID は CloudFront マネジメントコンソールにリンクされていることに注意してください。

Amazon CloudFront コンソールからディストリビューションに関する詳細情報にアクセスします。この情報へのアクセスについては、[「Amazon デベロッパーガイド」の「ディストリビューションの表示と更新」](#) を参照してください。 CloudFront

## ディストリビューションを編集する

CloudFront コンソールから Amazon CloudFront ディストリビューションを編集します。

AWS Elemental MediaPackage でオリジンを編集できるのは、MediaPackage でチャンネルにエンドポイントを追加するときにオリジンを作成する場合のみです。MediaPackage コンソールからディストリビューションを編集することはできません。

のディストリビューションにアクセスするには CloudFront、チャンネルの詳細ページでディストリビューションの ID を選択します。でのディストリビューションの編集の詳細については CloudFront、[「Amazon デベロッパーガイド」の「ディストリビューションの表示と更新」](#)を参照してください。 CloudFront

### Important

ディストリビューションを編集するときは、タグ付けページのデフォルトを変更しないでください。は、このタグのAWS Elemental MediaPackageチャンネル ID CloudFront を使用して、ディストリビューションとチャンネルをリンクします。タグが変更されると、MediaPackage からディストリビューションを表示したり管理したりできなくなります。

## ディストリビューションを削除する

CloudFront コンソールから Amazon CloudFront ディストリビューションを削除します。AWS Elemental MediaPackage コンソールでディストリビューションを削除することはできません。

のディストリビューションにアクセスするには CloudFront、チャンネルの詳細ページでディストリビューションの ID を選択します。でのディストリビューションの削除の詳細については CloudFront、[「Amazon CloudFront デベロッパーガイド」の「ディストリビューションの削除」](#)を参照してください。

# AWS Elemental MediaPackage のクォータ

以下のセクションでは、AWS Elemental MediaPackage のクォータについて説明します。

## トピック

- [ライブコンテンツのクォータ](#)
- [VOD コンテンツのクォータ](#)

## ライブコンテンツのクォータ

このセクションでは、AWS Elemental MediaPackage のライブコンテンツのクォータについて説明します。ソフトクォータの引き上げリクエストについては、「[AWS Service Quotas](#)」を参照してください。ハードクォータは変更できません。

## ライブのソフトクォータ

次の表では、ライブコンテンツに対する AWS Elemental MediaPackage のクォータで引き上げることができるものについて説明しています。クォータの変更については、「[AWS Service Quotas](#)」を参照してください。

一部のお客様のアカウントのクォータは、これらの公開されたクォータ以下である可能性があります。「リソース制限の超過」というエラーが誤って発生したと思われる場合は、Service Quotas コンソールを使用して[クォータの引き上げをリクエスト](#)します。

リソース	デフォルトのクォータ
チャンネルの最大数	30

### Note

チャンネルのクォータの引き上げは、必ずしもエンドポイント数の増加につながりません。たとえば、34 個のチャンネルが必要であり、各チャンネルで HLS、HLS 暗号化、DASH のコンテンツに対応する場合、各チャンネルに必要なエンドポイントは 3 つのみです (出

リソース	デフォルトのクォータ
	<p>カタイプごとに 1 つずつ)。デフォルトのエンドポイントのクォータは 10 であるため、チャンネルのクォータの引き上げは必要でも、エンドポイントのクォータの引き上げは不要です。チャンネルあたりのエンドポイントのクォータである 10 は超えません。</p>
チャンネルあたりのエンドポイントの最大数	<p>10</p> <p>これはチャンネルあたりのクォータです。各エンドポイントは、使用する出力パッケージを表します。1 つのチャンネルで HLS、HLS 暗号化、DASH、DASH 暗号化、Microsoft Smooth、および Microsoft Smooth 暗号化コンテンツに対応する場合、このチャンネルには 6 つのエンドポイントが必要です。これはエンドポイントのクォータである 10 以内の数です。同じ設定のチャンネルを 10 個に増やしても、各チャンネルのエンドポイント数は 6 のみであるため、クォータは超えません。</p>
同時に実行される収集ジョブの最大数	10
ライブマニフェストの最長時間	5 分

## ライブのハードクォータ

次の表では、ライブコンテンツに対する AWS Elemental MediaPackage のクォータで引き上げることができないものについて説明しています。

リソースまたはオペレーション	クォータ
チャンネルあたりの取り込みストリーム	チャンネルあたり 20 ストリーム



リソースまたはオペレーション	クォータ
タイムシフト表示の最大コンテンツ有効期間	336 時間 (14 日間)
タイムシフトマニフェストの最長時間	サポートされているすべての出力形式で 24 時間
Live-to-VOD マニフェストの最大長	サポートされているすべての出力形式で 24 時間
チャンネルあたりのリクエスト率	入力: 50 リクエスト/秒
エンドポイントあたりのリクエスト率	<ul style="list-style-type: none"> <li>メディアセグメント出力: 300 リクエスト/秒</li> <li>マニフェスト出力: 5000 リクエスト/秒</li> </ul> <div data-bbox="857 848 896 884" style="float: left; margin-right: 5px;">i</div> <div data-bbox="906 848 979 884">Note</div> <div data-bbox="906 905 1469 1608" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p>エンドポイントあたりのオリジネーションリクエスト率クォータはあくまでも目安であり、適切に設定された CDN を使用する場合の一般的なトラフィックパターンに基づいています。リクエスト率クォータは、ライブイベント、リニアチャンネル、タイムシフト表示に該当するものです。CDN の設定に誤りがある場合や、固有の HTTP ヘッダー値または再生 URL に追加された固有のクエリ文字列値を使用してプレイヤーが基準外レベルのオリジンリクエストを生成する場合など、特定の条件下ではリクエスト率クォータが低くなる可能性があります。</p> </div>
REST API のリクエスト数	<ul style="list-style-type: none"> <li>定常状態: 5 リクエスト/秒</li> <li>バースト状態: 50 リクエスト/秒</li> </ul>

リソースまたはオペレーション	クォータ
取り込みストリームあたりのトラック数	10  ストリームごとに取り込むことができるトラック (オーディオ、動画、字幕など) の最大数。

## VOD コンテンツのクォータ

このセクションでは、AWS Elemental MediaPackage のビデオオンデマンド (VOD) コンテンツのクォータについて説明します。ソフトクォータの引き上げリクエストについては、「[AWS Service Quotas](#)」を参照してください。ハードクォータは変更できません。

### VOD のソフトクォータ

次の表では、VOD コンテンツに対する AWS Elemental MediaPackage のクォータで引き上げることができるものについて説明しています。クォータの変更については、「[AWS Service Quotas](#)」を参照してください。

一部のお客様のアカウントのクォータは、これらの公開されたクォータ以下である可能性があります。「リソース制限の超過」というエラーが誤って発生したと思われる場合は、Service Quotas コンソールを使用して[クォータの引き上げをリクエスト](#)します。

リソース	デフォルトのクォータ
最大パッケージンググループ	10

#### Note

パッケージンググループのクォータを増やすことが、アセットやパッケージング設定を増やす必要があることを必ずしも意味するわけではありません。たとえば、14 個のグループが必要で、各アセットから HLS、HLS 暗号化、および DASH コンテンツを配信する場合は、各アセットに 3 つのパッケージ設

リソース	デフォルトのクォータ
	<p>定のみ (各出力タイプに 1 つ) が必要です。パッケージンググループあたりの設定数が 10 未満であるため、パッケージンググループ数のクォータを増やす必要はありますが、パッケージング設定のクォータを増やす必要はありません。</p>
<p>パッケージンググループあたりの最大パッケージング設定</p>	<p>10</p> <p>これはパッケージンググループあたりのクォータです。各パッケージ設定は、使用する出力パッケージを表します。1 つのパッケージンググループに HLS、HLS 暗号化、DASH、DASH 暗号化、Microsoft Smooth、および Microsoft Smooth の暗号化コンテンツの設定がある場合、そのグループには 6 つのパッケージ設定があり、10 の設定クォータ内にあります。同じ方法で 10 個のパッケージンググループを設定している場合でも、各グループは 6 つの設定しか使用しないため、まだクォータを超えていません。</p>
<p>最大アセット/パッケージンググループ</p>	<p>10,000</p> <p>これはパッケージンググループあたりのクォータです。たとえば、10,500 のアセットが複数のパッケージンググループにまたがっている場合でも、各グループのアセットが 10,000 以下であれば、クォータを超えることはありません。</p>

## VOD のハードクォータ

次の表では、VOD コンテンツに対する AWS Elemental MediaPackage のクォータで引き上げることができないものについて説明しています。

リソースまたはオペレーション	クォータ
アセットあたりの取り込みストリーム	20
アセットあたりのリクエスト率	<ul style="list-style-type: none"><li>メディアセグメント出力: 600 リクエスト/秒</li><li>マニフェスト出力: 1000 リクエスト/秒</li></ul> <div data-bbox="829 491 1507 1188"><p><b>Note</b></p><p>アセットあたりのオリジネーションリクエスト率クォータはあくまでも目安であり、適切に設定された CDN を使用した場合の一般的なトラフィックパターンに基づいています。CDN の設定に誤りがある場合や、固有の HTTP ヘッダー値または再生 URL に追加された固有のクエリ文字列値を使用してプレイヤーが基準外レベルのオリジンリクエストを生成する場合など、特定の条件下ではリクエスト率クォータが低くなることがあります。</p></div>
REST API のリクエスト数	<ul style="list-style-type: none"><li>定常状態: 5 リクエスト/秒</li><li>バースト状態: 50 リクエスト/秒</li></ul>
取り込みストリームあたりのトラック数	10  ストリームごとに取り込むことができるトラック (オーディオ、動画、字幕など) の最大数。

## AWS Elemental MediaPackage 関連情報

MediaPackage を利用する際に役立つ関連リソースを次の表にまとめました。

リソース	説明
<a href="#">クラスとワークショップ</a>	AWS に関するスキルを磨き、実践的な経験を積むために役立つ職務ベースのコース、専門コース、セルフペースラボへのリンクです。
<a href="#">AWS 開発者用ツール</a>	AWS アプリケーションの開発と管理のためのデベロッパーツール、SDK、IDE ツールキット、コマンドラインツールへのリンクです。
<a href="#">AWS ホワイトペーパー</a>	アーキテクチャ、セキュリティ、エコノミクスなどのトピックをカバーし、AWS のソリューションアーキテクトや他の技術エキスパートによって書かれた技術的な AWS ホワイトペーパーの包括的なリストへのリンクです。
<a href="#">AWS サポートセンター</a>	AWS サポートケースを作成および管理するためのハブ。フォーラム、技術上のよくある質問、サービスヘルスステータス、AWS Trusted Advisor などの便利なリソースへのリンクも含まれています。
<a href="#">AWS サポート</a>	1 対 1 での迅速な対応を行うサポートチャネルである AWS Support に関する情報のメインウェブサイトです。サポートは、クラウド上のアプリケーションの構築および実行を支援します。
<a href="#">お問い合わせ</a>	AWS の請求、アカウント、イベント、不正行為、他の問題などに関するお問い合わせの受付窓口です。

リソース	説明
<a href="#">AWS サイト規約</a>	当社の著作権、商標、お客様のアカウント、ライセンス、サイトへのアクセス、およびその他のトピックに関する詳細情報です。

## ユーザーガイドのドキュメント履歴

以下の表に、2018年5月以降の『AWS Elemental MediaPackage ユーザーガイド』の各リリースにおける重要な変更点を示します。このドキュメントの更新に関する通知を受け取るには、RSS フィードにサブスクライブできます。

- API バージョン: 最新

変更	説明	日付
<a href="#">ワークフローモニター</a>	AWS メディアサービスを分析し、それらのサービス間のシグナルマップ、つまりメディアワークフローの視覚化を作成します。シグナルマップを使用して、CloudWatch、EventBridgeを使用してモニタリングアラームと通知を生成します。AWS CloudFormation	2024年4月11日
<a href="#">DASH の新しいマニフェスト設定</a>	DRM トップレベルのコンパクトマニフェスト設定オプションを追加しました。	2024年1月26日
<a href="#">VOD の CMAF から cenc 暗号化オプションを削除</a>	SPEKE バージョン 2.0 を使用する VOD ワークフローの CMAF では、cbcs 暗号化のみがサポートされます。cenc 暗号化をテーブルから削除しました。	2023年4月24日
<a href="#">trickplay_type 値を追加</a>	none を含むよう trickplay_type を更新しました。これによりすべてのトリックプ	2023年4月24日

	レイトラックがフィルターされ れます。	
<a href="#">欠落している引用符を追加</a>	欠落していた終了引用符を例 に追加しました。	2023 年 4 月 24 日
<a href="#">SPEKE サポートを明確化</a>	プロトコルと DRM システム のサポートを明確にするため に SPEKE のテーブルを更新 しました。	2023 年 2 月 20 日
<a href="#">IAM ガイダンスを更新</a>	IAM ベストプラクティスに 沿ってガイドを更新しまし た。詳細については、「 <a href="#">IAM のセキュリティベストプラク ティス</a> 」を参照してくださ い。	2023 年 2 月 8 日
<a href="#">2 つのフィールドを削除</a>	コンソールからの削除に合わ せて、2 つのストリーム選択 フィールドを削除しました。	2023 年 1 月 5 日
<a href="#">タイプミスを修正</a>	「承認」のインスタンスを 「認証」に変更しました。	2022 年 12 月 19 日
<a href="#">I フレームのみのトリックプレ イのサポートを更新</a>	MediaPackage DASH VOD の I フレームのみのトリックプレ イをサポートするようになり ました。	2022 年 11 月 7 日
<a href="#">DASH の新しいマニフェスト 設定</a>	[I フレームのみのストリーム を含める] のマニフェスト設 定オプションが追加されまし た。	2022 年 11 月 7 日



<a href="#">trickplay_height と video_height クエリパラメータを更新</a>	Iフレームのみおよび画像ベースのトリックプレイを使用する際の trickplay_height と video_height クエリパラメータを更新しました。	2022 年 10 月 27 日
<a href="#">VOD とライブの両方で SPEKE バージョン 2.0 の対応を開始</a>	MediaPackage VOD CMAF と DASH ワークフローを備えた SPEKE バージョン 2.0 をサポートするようになりました。	2022 年 10 月 10 日
<a href="#">DASH の新しい SPEKE オプション</a>	MediaPackage VOD 用の DASH SPEKE バージョン 2.0 をサポートするようになりました。	2022 年 10 月 10 日
<a href="#">CMAF の新しい SPEKE オプション</a>	MediaPackage VOD 用の CMAF SPEKE バージョン 2.0 をサポートするようになりました。	2022 年 10 月 10 日
<a href="#">CMAF 暗号化の新しいオプション</a>	MediaPackage 暗号化された CMAF エンドポイントへの AES-CTR 暗号化をサポートするようになりました。	2022 年 9 月 2 日
<a href="#">SPEKE バージョン 2.0 のプリセットに関する情報を更新</a>	CPIX のバージョンが 2.3 に更新されました。プロトコルと DRM システムのサポートマトリックスを説明する SPEKE バージョン 2.0 のテーブルを更新しました。	2022 年 7 月 19 日

### [SPEKE バージョン 2.0 のプリセットに関する新しいドキュメント](#)

MediaPackage 暗号化されていないトラックと暗号化されたトラックの SPEKE バージョン 2.0 プリセット、すべてのオーディオトラックとビデオトラックの 1 つの暗号化キー、オーディオトラックとビデオトラック用の複数の暗号化キーをサポートします。

2022 年 7 月 19 日

### [新しい \[iFrame のみのストリームを含める\] オプション](#)

MediaPackage Include iFrame のみのストリームをサポートするようになり、マニフェスト内の他のトラックと一緒に iFrame のみのストリームを追加できるようになりました。

2022 年 7 月 19 日

### [マニフェストの更新時間](#)

MediaPackage 再生レスポンスには、MediaPackage マニフェストの最終更新日を指定するカスタムヘッダーが含まれるようになりました。

2022 年 1 月 3 日

### [HLS Live の画像ベースのトリックプレイに関する情報を追加する](#)

MediaPackage HLS Live のイメージベースのトリックプレイをサポートするようになりました。

2021 年 11 月 24 日

### [includeAudio パラメータのサポートを追加しました](#)

MediaPackage includeAudio .smil マニフェストでサポートされるようになりました。

2021 年 11 月 1 日

### [DVB 字幕の新しいオプション](#)

MediaPackage DVB 字幕をパッケージ設定出力に渡せるようになりました。

2021 年 10 月 20 日

<a href="#">DVB 字幕の新しいオプション</a>	MediaPackage DVB 字幕を HLS 出力にパススルーできるようになりました。	2021 年 10 月 20 日
<a href="#">新しいトリックプレイのトピック</a>	MediaPackage DASH のトリックプレイをサポートできるようになりました。	2021 年 10 月 15 日
<a href="#">アセット再生のステータス</a>	アセットでの再生準備状態に関するステータス情報を表示できるようになりました。これにより、アセットを再生する準備ができているかどうか、または処理が失敗したかどうかを確認できます。	2021 年 10 月 7 日
<a href="#">MediaPackage ライブワークフローで SPEKE バージョン 2.0 をサポートするようになりました。</a>	CMAF および DASH のライブワークフローでの SPEKE バージョン 2.0 に関する情報を追加しました。	2021 年 9 月 7 日
<a href="#">SPEKE バージョン 2.0 との統合に関する新しいガイダンス</a>	MediaPackage SPEKE バージョン 2.0 をサポートするようになりました。	2021 年 9 月 6 日
<a href="#">新しいメタデータパススルーのトピック</a>	MediaPackage ID3 と KLV のメタデータパススルーをサポートするようになりました。ID3 または KLV メタデータがチャンネルの入カストリームに存在する場合、MediaPackage そのメタデータは自動的に出カストリームに渡されます。	2021 年 6 月 30 日

<a href="#">CMAF 暗号化での新しいオプション</a>	MediaPackage CMAF パッケージ構成用に定数 IV と複数のシステム ID が提供されるようになりました。	2021 年 6 月 30 日
<a href="#">コスト配分タグ付けに関するコンテンツを更新</a>	コスト配分タグ付けの使用可能性を明確にしました。	2021 年 5 月 27 日
<a href="#">live-to-VOD の DASH エンドポイントを追加</a>	MediaPackage Live-to-VOD の DASH エンドポイント要件をサポートするようになりました。	2021 年 5 月 14 日
<a href="#">DASH と CMAF での新しいマニフェスト設定</a>	マニフェストの設定に、[Include encoder configuration in segments] (セグメントにエンコーダ構成を含める) オプションを追加しました。このオプションをオンにすると、シーケンスパラメータセット (SPS)、ピクチャーパラメータセット (PPS)、およびビデオパラメータセット (VPS) のメタデータは、init MediaPackage フラグメントではなく各ビデオセグメントに配置されます。	2021 年 4 月 28 日
<a href="#">audio_bitrate クエリパラメータを追加</a>	マニフェストのフィルタークエリ用のパラメータで、audio_bitrate が使用できるようになりました。	2021 年 3 月 22 日
<a href="#">アクセスのログ記録</a>	MediaPackage VOD のアクセスログをサポートするようになりました。	2021 年 2 月 24 日

<a href="#">MediaPackage イベントのイベント処理動作に関する情報を追加しました。CloudWatch</a>	MediaPackage CloudWatch ベストエフォート方式でイベントを送信します。	2021 年 1 月 7 日
<a href="#">アクセスのログ記録</a>	MediaPackage チャンネルへのリクエストの詳細な記録を提供するアクセスロギングをサポートするようになりました。これは、ライブワークフロー向けの機能です。	2020 年 10 月 21 日
<a href="#">DASH エンドポイントのための新しい UTC 計時オプション</a>	MediaPackage DASH エンドポイントの UTC タイミングをサポートするようになりました。	2020 年 10 月 20 日
<a href="#">SCTE-35 EXT-x-DATERANGE タグのサポート</a>	SCTE-35 広告マーカのトピックに、新たに EXT-X-DATERANGE セクションを追加しました。	2020 年 8 月 7 日
<a href="#">ライブマニフェストの最大長をハードクォータからソフトクォータに移動しました</a>	ライブマニフェストの最大長はソフトクォータとなりました。このエントリをハードクォータからソフトクォータに移動しました。	2020 年 6 月 24 日
<a href="#">VOD の CDN 認証に関する情報を追加</a>	CDN からのリクエストに認証を追加する方法を説明するために、トピック AWS Elemental MediaPackageでの CDN 認証を追加しました。	2020 年 5 月 29 日
<a href="#">マニフェストフィルタリングのトピックを更新</a>	6 つの新しいパラメータを追加し、文字数の制限を 1024 に更新しました。	2020 年 5 月 15 日

<a href="#">VOD タグ付けの制限を解除</a>	MediaPackage VOD のタグ付けをサポートするようになりました。	2020 年 4 月 23 日
<a href="#">新しいマニフェストフィルタリングのトピック</a>	新しいマニフェストフィルタリングのトピックが追加されました。	2020 年 4 月 8 日
<a href="#">タイムシフトおよび live-to-VOD のマニフェストの最長時間を更新</a>	サポートされるすべての出力形式で、マニフェストの最大長が 24 時間になりました。	2020 年 3 月 9 日
<a href="#">新しい VOD DASH-ISO マニフェストコンソール設定</a>	VOD パッケージ構成用の新しい DASH-ISO マニフェストコンソール設定を追加しました。コンパクト DASH、新しいセグメントテンプレート形式、期間トリガーのオプションが利用可能になりました。	2020 年 2 月 25 日
<a href="#">ライブと VOD の両方で複数期間の DASH の対応を開始</a>	複数期間 DASH の「ライブ専用」サポートへの参照を削除しました。	2020 年 2 月 25 日
<a href="#">VOD とライブの両方で圧縮 DASH マニフェストの対応を開始</a>	圧縮 DASH の「ライブ専用」サポートへの参照を削除しました。	2020 年 2 月 25 日
<a href="#">バグの修正</a>	CloudWatch 成功した収穫ジョブイベントが戻ります。 "status": "SUCCEEDED"	2020 年 2 月 10 日
<a href="#">CDN 認証に関する情報を追加しました。</a>	CDN からのリクエストに認証を追加する方法を説明するために、トピック AWS Elemental MediaPackageでの CDN 認証を追加しました。	2019 年 12 月 23 日

<a href="#">VOD 再生イベントに関する情報を追加</a>	取り込んだ VOD コンテンツの再生準備完了通知イベントの例を追加しました。	2019年11月8日
<a href="#">ライブから VOD CloudWatch へのイベントに関する情報を追加しました。</a>	live-to-VOD コンテンツ収集の収集ジョブ通知イベントの例を追加しました。	2019 年 10 月 15 日
<a href="#">.smil マニフェストに関する情報を追加</a>	VOD 取り込みでサポートされる .smil マニフェストの形式について説明する、「Requirements for .smil manifests」トピックを追加しました。	2019 年 10 月 10 日
<a href="#">live-to-VOD (ビデオオンデマンド) に関するトピックを追加</a>	ガイド全体で、「Live-to-VOD アセットの作成」や「Live-to-VOD コンテンツ配信」など、Live-to-VOD アセットの作成に関するトピックを追加および更新しました。	2019 年 10 月 1 日
<a href="#">タイムシフトマニフェストの時間制限を更新</a>	AWS Elemental MediaPackage コンパクトマニフェスト、HLS、CMAF を使用して DASH 用に最大 18 時間のタイムシフトマニフェストを作成できるようになりました。	2019 年 8 月 21 日
<a href="#">サポートされている入力と出力の情報を追加</a>	入力タイプ、コンテナ、コーデックがサポートする内容を説明する「サポートされている入力と出力」トピックを追加しました。 MediaPackage	2019 年 6 月 21 日

<a href="#">設定可能な SCTE-35 オプションを追加</a>	入力コンテンツに SCTE-35 AWS Elemental MediaPackage MediaPackage マーカーがある場合の動作を設定する方法を説明するトピックに SCTE-35 メッセージオプションを追加しました。	2019 年 6 月 21 日
<a href="#">セキュリティに関する章を追加しました。</a>	のセキュリティトピックを強化および標準化するために「セキュリティ」の章を追加しました。MediaPackage	2019 年 6 月 5 日
<a href="#">ビデオオンデマンド (VOD) のトピックを追加</a>	ガイド全体に、VOD コンテンツの処理に関するトピックを追加しました。VOD コンテンツ処理、Amazon Simple Storage Service MediaPackage へのアクセス許可、VOD コンテンツ配信、VOD コンテンツの配信、VOD コンテンツメトリクス、VOD コンテンツの制限などです。	2019 年 5 月 17 日
<a href="#">DASH マニフェスト形式オプションに関する詳細情報を追加しました。SegmentTemplate</a>	SegmentTimeline を使用する代わりに SegmentTemplate に期間情報を含める方法を説明するために、「Duration Attribute」トピックを追加しました。	2019 年 5 月 10 日
<a href="#">タイムシフトマニフェストの時間制限を更新</a>	AWS Elemental MediaPackage 最大 9 時間のタイムシフトマニフェストを作成できるようになりました。	2019 年 5 月 1 日



<a href="#">ライブおよび VOD のマニフェストに関する情報を追加</a>	ライブマニフェストまたは VOD MediaPackage マニフェストの配信時期を説明する「ライブおよび VOD マニフェストリファレンス」トピックを追加しました。	2019 年 4 月 16 日
<a href="#">タグ付けに関する情報を追加</a>	チャンネルとエンドポイントのタグ付けの仕組みを説明するタグングリソーストピックを追加しました。AWS Elemental MediaPackage	2019 年 3 月 4 日
<a href="#">DASH マニフェスト形式のオプションに関する情報を追加しました。SegmentTemplate</a>	DASH SegmentTemplate マニフェストのオブジェクト内のメディア URL の変数を変更する方法について説明する「DASH マニフェストセグメントテンプレートフォーマット」トピックを追加しました。	2019 年 2 月 6 日
<a href="#">DASH マニフェストの処理情報を追加</a>	出力 DASH マニフェストを変更する方法について説明するため、「DASH マニフェストオプション」トピックを追加しました。	2019 年 2 月 6 日
<a href="#">ログ情報を追加しました。AWS CloudTrail</a>	AWS Elemental MediaPackage API AWS CloudTrail CloudTrail のアクションをログに記録する方法について説明するトピックに Logging AWS Elemental MediaPackage API Calls を追加しました。	2018 年 12 月 21 日

### [圧縮 DASH マニフェストに関する情報を追加](#)

で DASH 出カマニフェストの圧縮がどのように機能するのかを説明する「圧縮された DASH マニフェスト」トピックを追加しました。AWS Elemental MediaPackage

2018 年 12 月 18 日

### [コンテンツ保持期間の制限を更新](#)

AWS Elemental MediaPackage コンテンツが 336 時間 (14 日間) 保持されるようになりました。

2018 年 11 月 13 日

### [DRM 暗号化にコンテンツキーの暗号化を追加](#)

コンテンツキーを暗号化するオプションが追加されました。これ以前は、AWS Elemental MediaPackage クリアキー配信のみをサポートしていました。コンテンツキーの暗号化を使用するには、DRM キープロバイダーが暗号化されたコンテンツキーをサポートしている必要があります。この機能をコンテンツキーの暗号化を扱えないキープロバイダーに対して有効にした場合、このオペレーションは失敗します。

2018 年 11 月 8 日

### [入力冗長の情報を追加](#)

バックアップ目的で 2 MediaPackage つの同一のストリームを受信する方法について説明する「入力冗長性の仕組み」トピックを追加しました。

2018 年 8 月 28 日

### [Amazon CloudFront コンソールの統合情報を追加](#)

AWS Elemental MediaPackage コンソールからディストリビューションを作成する方法など CloudFront、でのディストリビューションの操作に関するセクションを追加しました。

2018 年 8 月 3 日

### [複数期間の DASH に関する情報を追加](#)

AWS Elemental MediaPackageの複数期間 DASH のトピックを追加し、DASH マニフェストの複数期間について、目的と機能を説明しています。

2018 年 7 月 18 日

### [CDN に関する情報を追加](#)

Amazon などの CDN AWS Elemental MediaPackage との連携方法について説明する「CDN の操作」トピックを追加しました。CloudFront

2018 年 5 月 31 日

### [イベント通知の作成に関する情報を追加](#)

Amazon イベントと Amazon CloudWatch 簡易通知サービスを使用して新しいイベントを通知する方法を説明するイベント通知の作成トピックを追加しました。

2018 年 1 月 22 日

## 以前の更新

以下の表に、2018 年 5 月より前の『AWS Elemental MediaPackage ユーザーガイド』の各リリースにおける重要な変更点を示します。

変更	説明	日付
初版ドキュメントの作成	新規ドキュメント。	2017 年 11 月 27 日

変更	説明	日付
リンクを修正してホワイトリストを追加	<p>AWS Elemental MediaPackage コンソールと AWS Elemental MediaPackage API リファレンスへのリンクを修正しました。</p> <p>「エンドポイントの使用」に、アクセスコントロールフィールドのリファレンスを追加しました。</p>	2017 年 12 月 1 日
固有の IAM ポリシー情報を追加しました。AWS Elemental MediaPackage	「 <a href="#">セットアップ MediaPackage</a> 」に、アクセス権限が制限された管理者以外のロールの作成手順を追加しました。	2017 年 13 月 12 日
ハード制限情報を追加	「 <a href="#">AWS Elemental MediaPackage のクォータ</a> 」に、変更できない制限 (ハード制限) に関する情報を追加しました。	2017 年 12 月 20 日
IAM ポリシー情報を更新	に <a href="#">セットアップ MediaPackage</a> 、固有のポリシーに関する情報を追加しました。AWS Elemental MediaPackage	2018 年 1 月 5 日
CMAF エンドポイントに関する情報を追加	新しい出力タイプに関する「 <a href="#">CMAF エンドポイントの作成</a> 」セクションを追加しました。	2018 年 4 月 6 日
機能の説明を更新	「 <a href="#">AWS Elemental MediaPackage の機能</a> 」に、HDR-10 のサポート機能を追加しました。	2018 年 30 月 4 日

変更	説明	日付
CDN に関する情報を追加	Amazon CloudFront などの CDN <a href="#">CDN の使用</a> AWS Elemental MediaPackage との連携方法について説明するトピックを追加しました。	2018 年 5 月 31 日

#### Note

- AWS メディアサービスは、生命安全運用、ナビゲーションシステム、通信システム、航空管制、生命維持装置など、サービスの利用不能、中断、または障害により死亡、人身傷害、物的損害、または環境被害につながる可能性があるフェイルセーフ性能を必要とするアプリケーションや状況での使用を意図したものではありません。

# AWS 用語集

AWS の最新の用語については、「AWS の用語集リファレンス」の「[AWS 用語集](#)」を参照してください。

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