

パートナーおよびカスタマーガイド

Secure Packager と Encoder Key Exchange APIの仕様



Secure Packager と Encoder Key Exchange API の仕様: パートナーおよびカスタマーガイド

Copyright © 2021 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは、Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していない他のすべての商標は、それぞれの所有者の所有物であり、Amazon と提携、接続、または後援されている場合とされていない場合があります。

Table of Contents

Secure Packager and Encoder Key Exchange とは	1
全般的アーキテクチャ	1
AWS クラウドベースのアーキテクチャ	2
開始方法	3
SPEKE を初めて利用する場合	4
関連するサービス情報と仕様	4
用語	4
顧客オンボーディング	6
DRM プラットフォームプロバイダーの使用を開始する	6
SPEKE AWSサービスと製品でのサポート	7
SPEKE AWSパートナーサービスと製品でのサポート	8
SPEKE API 仕様	9
に必要な認証 SPEKE	10
AWS クラウド実装の認証	10
オンプレミス製品の認証	11
SPEKE API v1	12
SPEKE API v1 - DASH-IF 仕様のカスタマイズと制約	13
SPEKE API v1 - 標準ペイロードコンポーネント	14
SPEKE API v1 - ライブワークフローメソッド呼び出しの例	16
SPEKE API v1 - VOD ワークフローメソッド呼び出しの例	21
SPEKE API v1 - コンテンツキーの暗号化	24
SPEKE API v1 - ハートビート	28
SPEKE API v1 - キー識別子の上書き	28
SPEKE API v2	30
SPEKE API v2 - DASH-IF 仕様のカスタマイズと制約	31
SPEKE API v2 - 標準ペイロードコンポーネント	35
SPEKE API v2 - 暗号化契約	40
SPEKE API v2 - ライブワークフローメソッド呼び出しの例	50
SPEKE API v2 - VOD ワークフローメソッド呼び出しの例	56
SPEKE API v2 - コンテンツキーの暗号化	61
SPEKE API v2 - キー識別子の上書き	65
SPEKE API 仕様のライセンス	66
Creative Commons Attribution-ShareAlike 4.0 国際パブリックライセンス	66
ドキュメント履歴	74

..... lxxviii

Secure Packager and Encoder Key Exchange とは

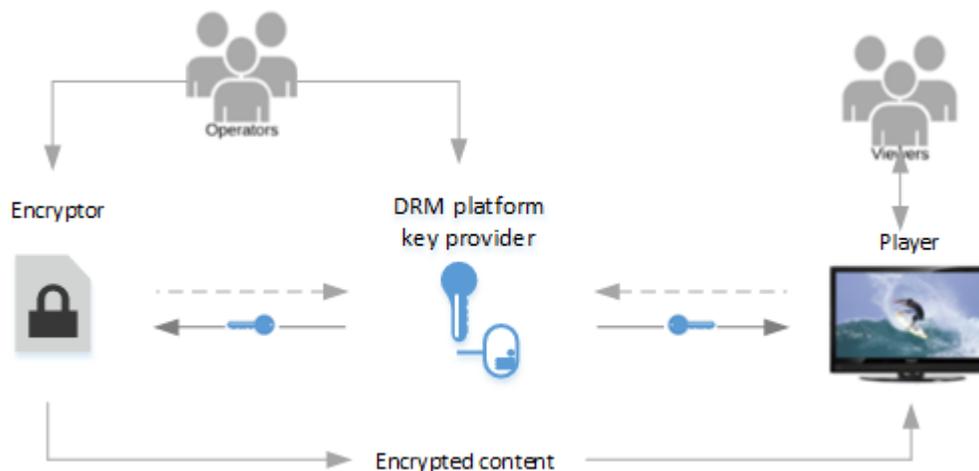
Secure Packager and Encoder Key Exchange (SPEKE) は、メディアコンテンツのエンクリプタとパッケージャ、およびデジタル著作権管理 (DRM) キープロバイダー間の通信の標準を定義します。この仕様は、オンプレミスおよび AWS クラウドで実行されているエンクリプタに対応しています。

トピック

- [全般的アーキテクチャ](#)
- [AWS クラウドベースのアーキテクチャ](#)
- [開始方法](#)

全般的アーキテクチャ

次の図は、オンプレミス製品のSPEKEコンテンツ暗号化アーキテクチャの概要を示しています。

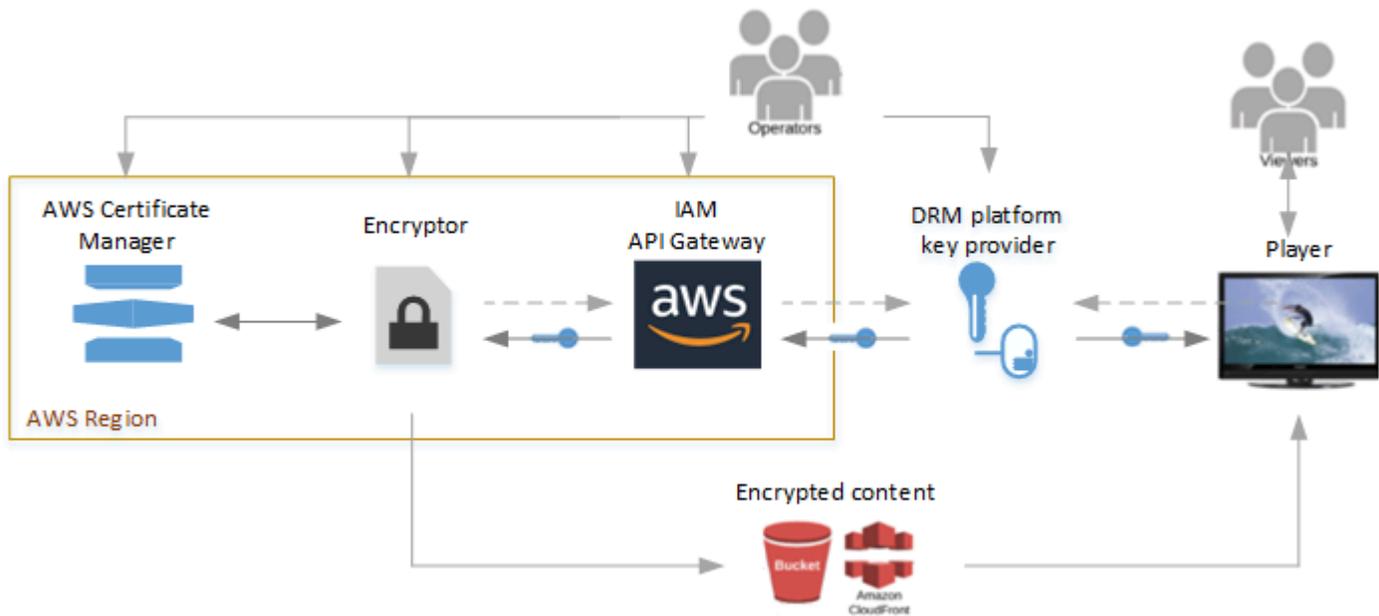


これらが、上記のアーキテクチャの主なコンポーネントです。

- エンクリプタ – 暗号化技術を提供します。オペレーターから暗号化リクエストを受信し、暗号化されたコンテンツを保護するためにキープロバイダーから必要なDRMキーを取得します。
- DRM プラットフォームキープロバイダー – SPEKE準拠の を介して暗号化キーをエンクリプタに提供しますAPI。メディアプレイヤーに復号化のためのライセンスも提供します。
- Player – 同じDRMプラットフォームキープロバイダーからキーをリクエストします。プレイヤーはこれを使用してコンテンツのロックを解除し、ビューワーに提供します。

AWS クラウドベースのアーキテクチャ

次の図SPEKEは、AWS クラウドで実行されている のサービスや機能で を使用する場合の高レベルのアーキテクチャを示しています。



以下に主なサービスとコンポーネントを示します。

- **エンクリプタ** — AWS クラウドで暗号化テクノロジーを提供します。エンクリプタは、オペレータからリクエストを受け取り、暗号化されたコンテンツを保護するために、Amazon API Gateway を介してキープロバイダーから必要な暗号化DRMキーを取得します。暗号化されたコンテンツを Amazon S3 バケットまたは Amazon CloudFront デイストリビューション経由で配信します。
- **AWS IAM および Amazon API Gateway** – エンクリプタとキープロバイダー間の顧客信頼のロールとプロキシ通信を管理します。API Gateway はログ機能を提供し、お客様がエンクリプタおよびプラットフォームとの関係を制御できるようにします。お客様は、IAMロール設定を通じてキープロバイダーアクセスを有効にします。API ゲートウェイはエンクリプタと同じAWSリージョンに存在する必要があります。
- **AWS Certificate Manager** – (オプション) コンテンツキー暗号化の証明書管理を提供します。コンテンツキーの暗号化は、安全な通信のために推奨されるプラクティスです。証明書マネージャーは、エンクリプタと同じAWSリージョンに存在する必要があります。
- **DRM プラットフォームキープロバイダー** – SPEKE準拠の を介して暗号化キーをエンクリプタに提供しますAPI。メディアプレイヤーに復号化のためのライセンスも提供します。
- **Player** – 同じDRMプラットフォームキープロバイダーからキーをリクエストします。プレイヤーはこれを使用してコンテンツのロックを解除し、ビューワーに配信します。

開始方法

に関するその他の入門資料についてはSPEKE、[「を初めて使用する場合SPEKE」](#)を参照してください。

お客様の場合

Elemental AWS DRMプラットフォームプロバイダーと提携して、暗号化を使用するようにセットアップします。詳細については、[顧客オンボーディング](#)を参照してください。

DRMプラットフォームプロバイダーですか、それとも独自のキープロバイダーの顧客ですか。

SPEKE仕様に従ってキープロバイダーRESTAPIのを公開します。詳細については、「[SPEKEAPI仕様](#)」を参照してください。

SPEKE を初めて利用する場合

このセクションでは、Secure Packager and Encoder Key Exchange () を初めて使用する場合の入門情報を提供しますSPEKE。

の概要についてはSPEKE、次のウェブキャストをご覧ください。

関連するサービス情報と仕様

- [API ゲートウェイのアクセス許可](#) – AWS Identity and Access Management (AWSIAM) のアクセス許可APIを使用してへのアクセスを制御する方法。
- [AWS AssumeRole](#) – AWS Security Token Service (AWS STS) を使用してロール機能を引き受ける方法。
- [AWS Sigv4](#) – 署名バージョン 4 を使用してHTTPリクエストに署名する方法。
- [DASH-IF CPIX仕様 v2.0](#) – この v1.0 仕様に基づいている DASH-IF Content Protection Information Exchange Format (CPIX) SPEKE 仕様バージョン。
- [DASH-IF CPIX仕様 v2.3](#) – この v2.0 仕様に基づいている DASH-IF コンテンツ保護情報交換形式 (CPIX) SPEKE 仕様バージョン。
- [DASH-IF システム IDs](#) – DRMシステムの登録済み識別子のリスト。
- <https://github.com/awslabs/speke-reference-server> – でのSPEKE実装を開始するのに役立つ、AWS アカウントで使用するリファレンスキープロバイダーの例AWS。

用語

次のリストは、この仕様で使用される用語を定義します。可能な場合、この仕様は [DASH-IF CPIX仕様](#) で使用される用語に従います。

- ARN – Amazon リソースネーム。AWS リソースを一意に識別します。
- コンテンツキー – コンテンツの一部を暗号化するために使用される暗号化キー。
- コンテンツプロバイダー – 保護されたメディアを配信するためのルールと権利を提供するパブリッシャー。コンテンツプロバイダーは、ソースメディア (トランスコード用のメザン形式)、アセット識別子、キー識別子 (KIDs)、キー値、エンコーディング手順、コンテンツ説明メタデータを提供する場合もあります。

- DRM – デジタル著作権管理。著作権で保護されているデジタルコンテンツを未承認のアクセスから保護するために使用されます。
- DRM プラットフォーム – コンテンツの暗号化と復号のためのDRMキーとライセンスの提供など、コンテンツエンクリプタとビューワーにDRM機能とサポートを提供するシステム。
- DRM provider – DRMプラットフォームを参照してください。
- DRM system – DRM実装の標準。一般的なDRMシステムには、Apple FairPlay、Google Widevine、Microsoft などがあります PlayReady。DRM システムは、ビューワーへの配信とビューワーによるアクセスのためにデジタルコンテンツを保護するために、コンテンツプロバイダーによって使用されます。DASH-IF に登録されているDRMシステムのリストについては、[DASH 「-IF system IDs」](#) を参照してください。[DASH-IF CPIX仕様](#)は、ここで定義されている「system」という用語DRMを使用しDRM、場合によっては「system」を使用して、この仕様がDRMプラットフォームと呼ぶものを意味します。
- DRM ソリューション – DRM「プラットフォーム」を参照してください。
- DRM テクノロジー – DRMシステムを参照してください。
- エンクリプタ – キープロバイダから取得したキーを使用してメディアコンテンツを暗号化するメディア処理コンポーネント。通常、暗号化シDRMグナリングとメタデータもメディアに追加します。エンクリプタは通常、エンコーダー、パッケージャー、トランスコーダーです。
- キープロバイダー – キーリクエストを処理するSPEKERESTAPIために を公開するDRMプラットフォームのコンポーネント。キープロバイダーは、キーサーバー自体であるか、プラットフォームの別のコンポーネントである場合があります。
- キーサーバー – コンテンツの暗号化と復号のためのキーを維持するDRMプラットフォームのコンポーネント。
- オペレーター – エンクリプタやキープロバイダーを含め、システム全体の運用の担当者。
- プレイヤー – ビューワーに代わって動作するメディアプレイヤー。メディアマニフェストファイル、メディアファイル、DRMライセンスなど、さまざまなソースから情報を取得します。ビューワーに代わってDRMプラットフォームからライセンスをリクエストします。

のカスタマーオンボーディング SPEKE

Secure Packager および Encoder Key Exchange (SPEKE) デジタル著作権管理 (DRM) キープロバイダーを暗号化ツールとメディアプレイヤーと組み合わせることで、コンテンツを不正使用から保護します。SPEKE は、メディアコンテンツの暗号化者とパッケージ化者、およびデジタル著作権管理 (DRM) キープロバイダー間の通信の標準を定義します。オンボードするには、DRMプラットフォームキープロバイダーを選択し、キープロバイダーと暗号化子およびプレイヤー間の通信を設定します。

トピック

- [DRM プラットフォームプロバイダーの使用を開始する](#)
- [SPEKE AWSサービスと製品でのサポート](#)
- [SPEKE AWSパートナーサービスと製品でのサポート](#)

DRM プラットフォームプロバイダーの使用を開始する

次の Amazon パートナーは、のサードパーティーDRMプラットフォーム実装を提供します SPEKE。提供サービスに関する詳細とお問い合わせ方法については、Amazon パートナーネットワークのページへのリンクをクリックしてください。リンクがないパートナーには現在 Amazon パートナーネットワークのページがありませんが、直接連絡することができます。パートナーからは、パートナーが提供するプラットフォームを使用するためのセットアップのサポートを受けられません。

DRM プラットフォームプロバイダー	SPEKE v1 サポート	SPEKE v2 サポート
Axinom	√	√
購入DRM	√	√
castLabs	√	√
EZDRM	√	√
Inisoft	√	√
INKA エントリ	√	√

DRM プラットフォームプロバイダー	SPEKE v1 サポート	SPEKE v2 サポート
Insys クラウド DRM	√	√
Intertrust Technologies	√	√
Irdeto	√	√
JW Player	√	√
Kaltura	√	
NAGRA	√	√
NEXTSCAPE株式会社	√	√
SeaChange	√	
Verimatrix	√	√
Viaccess-Orca	√	
WebStream	√	√

SPEKE AWSサービスと製品でのサポート

このセクションでは、AWS クラウドで実行される AWS Media Services とAWSオンプレミスのメディア製品が提供するSPEKEサポートを一覧表示します。これらのサービスと製品は、SPEKEコンテンツ暗号化アーキテクチャの暗号化子です。ストリーミングプロトコルと、サービスまたは製品で必要なDRMシステムが使用可能であることを確認します。

AWS サービスまたは製品	SPEKE v1 サポート	SPEKE v2 サポート	サポートされているDRMテクノロジー
AWS Elemental MediaConvert - AWS クラウドで実行されるサービス	√	√	ドキュメント

AWS サービスまたは製品	SPEKE v1 サポート	SPEKE v2 サポート	サポートされている DRMテクノロジー
AWS Elemental MediaPackage - AWS クラウドで実行されるサービス	√	√	ドキュメント
AWS Elemental Live - オンプレミス製品	√		ドキュメント: MPEG-DASH / HLS
AWS Elemental Server - オンプレミス製品	√		ドキュメント

SPEKE AWSパートナーサービスと製品でのサポート

このセクションでは、AWS クラウドで実行されるAWSパートナーサービスと製品が提供するSPEKEサポートを一覧表示します。これらのサービスと製品は、SPEKEコンテンツ暗号化アーキテクチャの暗号化子です。ストリーミングプロトコルと、サービスまたは製品に必要なDRMシステムが使用可能であることを確認します。

AWS サービスまたは製品	SPEKE v1 サポート	SPEKE v2 サポート	サポートされている DRMテクノロジー
Bitmovin Live Video Encoding	√		ドキュメント
Bitmovin Video on demand (VOD) エンコーディング	√		ドキュメント

SPEKE API 仕様

これは Secure Packager and Encoder Key Exchange () のRESTAPI仕様ですSPEKE。この仕様を使用して、暗号化を使用するお客様にDRM著作権保護を提供します。

ビデオストリーミングワークフローでは、暗号化エンジンはDRMプラットフォームキープロバイダーと通信してコンテンツキーをリクエストします。これらのキーは非常に機密性が高いため、キープロバイダーと暗号化エンジンが安全性と信頼性の高い通信チャネルを確立することが重要です。ドキュメント内のコンテンツキーを暗号化して、より安全で end-to-end 暗号化することもできます。

この仕様では、次の目標に対応しています。

- DRM ベンダーや顧客がコンテンツの暗号化が必要な場合にエンクリプタと統合するために使用できる、シンプルで信頼され、安全性の高いインターフェイスを定義します。
- VOD およびライブワークフローをカバーし、エンクリプタとDRMキープロバイダーエンドポイント間の堅牢で安全性の高い通信に必要なエラー条件と認証メカニズムを含めます。
- HLS、MSS、および DASHパッケージとその共通DRMシステムのサポートを含めます。FairPlay、PlayReady、および Widevine/CENC。
- 将来のDRMシステムをサポートするために、仕様をシンプルかつ拡張可能に保ちます。
- シンプルな REST を使用しますAPI。

Note

Copyright 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ドキュメントは、クリエイティブコモンズ属性-ShareAlike 4.0 国際ライセンスで入手できます。

THE MATERIAL CONTAINED HEREIN は、PROVIDED 「AS IS」、WITHOUT WARRANTY の ANY KIND、EXPRESS または IMPLIED INCLUDING BUT NOT LIMITED から THE WARRANTIES MERCHANTABILITY、 PARTICULAR PURPOSE AND FITNESS FOR での NON-INFRINGEMENT。の EVENT SHALL THE AUTHORS、 COPYRIGHT HOLDERS の THIS MATERIAL LIABLE FOR ANY CLAIM DAMAGES、 、 WHETHER の OTHER LIABILITY、 CONTRACT、 ACTION の OTHERWISE、 ARISING OUT の TORT FROM、 の 、 の CONNECTION WITH THIS MATERIAL、 の THE USE、 または THIS OTHER DEALINGS の はありません MATERIAL。

トピック

- [に必要な認証 SPEKE](#)
- [SPEKE API v1](#)
- [SPEKE API v2](#)
- [SPEKE API 仕様のライセンス](#)

に必要な認証 SPEKE

SPEKE では、オンプレミス製品と、AWS クラウドで実行される のサービスおよび機能の認証が必要です。

トピック

- [AWS クラウド実装の認証](#)
- [オンプレミス製品の認証](#)

AWS クラウド実装の認証

SPEKE エンクリプタで使用するには、IAMロールによるAWS認証が必要です。IAM ロールは、DRMプロバイダーまたはAWSアカウントのDRMエンドポイントを所有するオペレーターによって作成されます。各ロールには Amazon リソースネーム (ARN) が割り当てられ、Elemental AWS サービスオペレーターは暗号化をリクエストするときにサービスコンソールでこれを提供します。ロールのポリシーのアクセス許可は、キープロバイダーにアクセスするためのアクセス許可を付与 APIし、他のAWSリソースにアクセスしないように設定する必要があります。エンクリプタがDRM キープロバイダーに連絡すると、ロールを使用してキープロバイダーアカウント所有者のロールを ARN引き受けます。これにより、エンクリプタがキープロバイダーにアクセスするために使用する一時的な認証情報が返されます。

一般的な実装の 1 つは、オペレーターまたはDRMプラットフォームベンダーがキープロバイダーの前に Amazon API Gateway を使用し、APIゲートウェイリソースで AWS Identity and Access Management (AWS IAM) 認証を有効にすることです。次のポリシー定義の例を使用し、新しいロールにアタッチして、適切なリソースにアクセス権限を与えることができます。この場合、アクセス許可はすべてのAPIゲートウェイリソースに対するものです。

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


SPEKE API v1

これは、Secure Packager and Encoder Key Exchange (SPEKE) v1 RESTAPI用のです。この仕様を使用して、暗号化を使用するお客様にDRM著作権保護を提供します。SPEKEに準拠するには、DRMキープロバイダーがこの仕様でRESTAPI説明されている を公開する必要があります。エンクリプタはキープロバイダーをAPI呼び出します。

Note

この仕様のコード例は、あくまでも説明用です。サンプルは完全なSPEKE実装の一部ではないため、実行することはできません。

SPEKE は、DASHIndustry Forum Content Protection Information Exchange Format (DASH-IF-CPIX) データ構造定義をキー交換に使用しますが、いくつかの制限があります。DASH-IF-CPIX は、DRMプラットフォームからエンクリプタへの拡張可能なマルチDRMエクスチェンジを提供するスキーマを定義します。これにより、コンテンツの圧縮およびパッケージング時に、すべての適応ビットレートパッケージング形式のコンテンツ暗号化が可能になります。アダプティブビットレートパッケージング形式にはHLS、DASH、およびが含まれますMSS。

交換形式の詳細については、<https://dashif.org/docs/DASH-IF--v2CPIX-0.pdf> のDASH「Industry Forum CPIX仕様」を参照してください。

トピック

- [SPEKE API v1 - DASH-IF 仕様のカスタマイズと制約](#)
- [SPEKE API v1 - 標準ペイロードコンポーネント](#)
- [SPEKE API v1 - ライブワークフローメソッド呼び出しの例](#)
- [SPEKE API v1 - VOD ワークフローメソッド呼び出しの例](#)
- [SPEKE API v1 - コンテンツキーの暗号化](#)
- [SPEKE API v1 - ハートビート](#)
- [SPEKE API v1 - キー識別子の上書き](#)

SPEKE API v1 - DASH-IF 仕様のカスタマイズと制約

DASH-IF CPIX仕様 <https://dashif.org/docs/DASH-IF-CPIX-v2-0.pdf> は、多くのユースケースとトポロジをサポートしています。SPEKE API 仕様は、以下のカスタマイズと制約によりCPIX仕様に準拠しています。

- SPEKE は、エンクリプタコンシューマーのワークフローに従います。
- 暗号化されたコンテンツキーの場合、 は次の制限SPEKEを適用します。
 - SPEKE は、リクエストまたはレスポンスペイロードのデジタル署名検証 (XMLDSIG) をサポートしていません。
 - SPEKE には 2048 RSAベースの証明書が必要です。
- ローテーションキーワークフローの場合、 にはContentKeyUsageRuleフィルター SPEKEが必要ですKeyPeriodFilter。SPEKE は、他のすべてのContentKeyUsageRule設定を無視します。
- SPEKE は UpdateHistoryItemList の機能を省略します。リストがレスポンスに存在する場合、 はそのリストSPEKEを無視します。
- SPEKE はキーローテーションをサポートします。SPEKE は ContentKeyPeriod`@index`のみを使用してキー期間を追跡します。
- をサポートするためにMSS PlayReady、 はDRMSystemタグ の下にカスタムパラメータ SPEKEを使用しますSPEKE:ProtectionHeader。
- HLS パッケージングでは、 URIExtXKeyがレスポンスに存在する場合、 HLSプレイリストの EXT-X-KEY タグの URIパラメータに追加する完全なデータを含める必要があります。これ以上のシグナリングは必要ありません。
- HLS プレイリストの場合、 DRMSystem タグの下には、 EXT-X-KEYタグの speke:KeyFormatおよび パラメータの値にspeke:KeyFormatVersionsオプションのカスタムKEYFORMATVERSIONSパラメータ KEYFORMATおよび SPEKEが用意されています。

HLS 初期化ベクトル (IV) は、 演算子によって明示的に指定されない限り、常にセグメント番号に従います。

- キーをリクエストするとき、エンクリプタは、ContentKey 要素にオプションの @explicitIV 属性を使用することがあります。キープロバイダーは、属性がリクエストに含まれていなくても、@explicitIV を使用して IV で応答することができます。
- エンクリプタはキー識別子 (KID) を生成しますが、これは与えられたコンテンツ ID とキー期間に対して同じです。キープロバイダーには、リクエストドキュメントに対するレスポンスとして KID が含まれます。

- キープロバイダーには、デバッグ目的のために自身を識別する、Speke-User-Agent レスポンスヘッダーの値を含めることができます。
- SPEKE は現在、コンテンツごとに複数のトラックまたはキーをサポートしていません。

SPEKE 準拠のエンクリプタはクライアントとして機能し、キープロバイダーエンドポイントに POST オペレーションを送信します。エンクリプタは定期的に heartbeat リクエストを送信して、エンクリプタとキープロバイダーエンドポイントとの間の接続が正常であることを確認する場合があります。

SPEKE API v1 - 標準ペイロードコンポーネント

どの SPEKE リクエストでも、エンクリプタは 1 つ以上の DRM システムのレスポンスをリクエストできます。エンクリプタは、リクエストペイロード <cpix:DRMSystemList> の内の DRM システムを指定します。各システム仕様には、キーが含まれており、返されるレスポンスのタイプを示します。

次の例は、単一の DRM システム仕様を持つ DRM システムリストを示しています。

```
<cpix:DRMSystemList>
  <!-- HLS AES-128 (systemId is implementation specific)-->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
    systemId="81376844-f976-481e-a84e-cc25d39b0b33">
    <cpix:URIEExtXKey></cpix:URIEExtXKey>
    <speke:KeyFormat></speke:KeyFormat>
    <speke:KeyFormatVersions></speke:KeyFormatVersions>
  </cpix:DRMSystem>
</cpix:DRMSystemList>
```

次の表は、各 <cpix:DRMSystem> の主要コンポーネントを示しています。

識別子	説明
systemId、または schemeId	IF DASH 組織に登録されている DRM システムタイプの一意の識別子。リストについては、 DASH 「-IF System IDs」 を参照してください。
kid	キー ID。これは実際のキーではなく、ハッシュテーブルのキーを指す識別子です。

識別子	説明
<cpix:UriExtXKey>	標準の暗号化されていないキーをリクエストします。キーレスポンスタイプはこれが、PSSHレスポンスのいずれかである必要があります。
<cpix:PSSH>	Protection System Specific Header () をリクエストしますPSSH。このタイプのヘッダーにはkid、共通暗号化 () の一部として、systemID、およびDRMベンダーのカスタムデータへの参照が含まれていますCENC。キーレスポンスタイプはこれが、UriExtXKey レスポンスのいずれかである必要があります。

標準キーと PSSH のリクエスト例

次の例は、エンクリプタからDRMキープロバイダーへのサンプルリクエストの一部を示し、主なコンポーネントが強調表示されています。最初のリクエストは標準キー用で、2番目のリクエストはPSSHレスポンス用です。

```
<cpix:CPIX id="abc123" xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc" xmlns:speke="urn:aws:amazon:com:speke">
  <cpix:ContentKeyList>
    <cpix:ContentKey kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
explicitIV="OFj2IjCsPJFfMAxmQxLGPw=="></cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- HLS AES-128 (systemId is implementation specific)-->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" ← KID
systemId="81376844-f976-481e-a84e-cc25d39b0b33"> ← System Id
      <cpix:UriExtXKey></cpix:UriExtXKey> ← request Key
      <speke:KeyFormat></speke:KeyFormat>
      <speke:KeyFormatVersions></speke:KeyFormatVersions>
    </cpix:DRMSystem>

    <!-- Common encryption (Widevine)-->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" ← KID
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed"> ← System Id
      <cpix:PSSH></cpix:PSSH> ← request PSSH
    </cpix:DRMSystem>
  </cpix:DRMSystemList>
  ...
</cpix:CPIX>
```

標準キーと PSSH のレスポンスの例

次の例は、DRMキープロバイダーからエンクリプタへの対応するレスポンスを示しています。

```
<cpix:CPIX xmlns:cpix="urn:dashif:org:cpix" xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
xmlns:speke="urn:aws:amazon:com:speke" id="abc123">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="OFj2IjCsPJFFmAxmQxLGPw=="
      kid="98ee5596-cd3e-a20d-163a-e382420c6eff">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- HLS AES-128 (systemId is implementation specific) -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" ← KID
      systemId="81376844-f976-481e-a84e-cc25d39b0b33"> ← System Id
      <cpix:URIExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWNldGUtYXBpLnVzLXdlc3QtMi5hbWV6b25hd3M
      uY29tL0VrZVN0YVdlL2N5aWVudC9hYmMxMjMvOThlZTU1OTYtY2QzZS1hMjBkLWTE2M2EtZTM4MjQyMGM2ZWZ
      m</cpix:URIExtXKey> ← Key
      <speke:KeyFormat>aWRlbnRpdHk=</speke:KeyFormat>
      <speke:KeyFormatVersions>MQ==</speke:KeyFormatVersions>
    </cpix:DRMSystem>

    <!-- Common encryption (Widevine) -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" ← KID
      systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed"> ← System Id
      <cpix:PSSH>AAAAanBzc2gAAAAA7e+LqXnWSs6jyCfc1R0h7QAAAEoIARIQeSIcblaNbb7Dji6sAtKzRoNd
      2lkZXZpbmVfdGVzdCIfa2V5LWlkOmVTSWNibGFOYmI3RGppNnNBdEtaelE9P8oCU0QyAA==</cpix:PSSH> ← PSSH
    </cpix:DRMSystem>
  </cpix:DRMSystemList>
  ...
</cpix:CPIX>
```

SPEKE API v1 - ライブワークフローメソッド呼び出しの例

リクエストの構文例

以下はURL例であり、固定形式を示すものではありません。

```
POST https://speke-compatible-server/speke/v1.0/copyProtection
```

リクエストボディ

CPIX 要素。

リクエストヘッダー

名前	型	発生	説明
AWS Authoriza tion	文字列	1..1	AWS Sigv4 を参照
X-Amz-Security- Token	文字列	1..1	AWS Sigv4 」 を参照
X-Amz-Date	文字列	1..1	AWS Sigv4 を参照
Content-Type	文字列	1..1	application/xml

レスポンスヘッダー

名前	型	発生	説明
Speke-User- Agent	文字列	1..1	キープロバイダーを 識別する文字列
Content-Type	文字列	1..1	application/xml

レスポンスのリクエスト

HTTP CODE	ペイロード名	発生	説明
200 (Success)	CPIX	1..1	DASH-CPIX ペイロー ドレスポンス
4XX (Client error)	クライアントエラー メッセージ'	1..1	クライアントエラー の説明
5XX (Server error)	サーバーエラーメッ セージ	1..1	サーバーエラーの説 明

Note

このセクションの例には、コンテンツキーの暗号化は含まれていません。コンテンツキーの暗号化を追加する方法については、[コンテンツキーの暗号化](#)を参照してください。

クリアでキーを含むリクエストペイロードのライブ例

次の例は、エンクリプタからDRMキープロバイダーへの一般的なライブリクエストペイロードを示しています。

```
<cpix:CPIX id="abc123" xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
  xmlns:speke="urn:aws:amazon:com:speke">
  <cpix:ContentKeyList>
    <cpix:ContentKey kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  explicitIV="0Fj2IjCsPJFfMAxmQxLGPw=="></cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- HLS AES-128 (systemId is implementation specific)-->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="81376844-
  f976-481e-a84e-cc25d39b0b33">
      <cpix:URIEExtXKey></cpix:URIEExtXKey>
      <speke:KeyFormat></speke:KeyFormat>
      <speke:KeyFormatVersions></speke:KeyFormatVersions>
    </cpix:DRMSystem>

    <!-- HLS SAMPLE-AES -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
      <cpix:URIEExtXKey></cpix:URIEExtXKey>
      <speke:KeyFormat></speke:KeyFormat>
      <speke:KeyFormatVersions></speke:KeyFormatVersions>
    </cpix:DRMSystem>

    <!-- Common encryption (Widevine)-->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
      <cpix:PSSH></cpix:PSSH>
    </cpix:DRMSystem>

    <!-- Common encryption / MSS (Playready) -->
```

```

<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
  <speke:ProtectionHeader></speke:ProtectionHeader>
  <cpix:PSSH></cpix:PSSH>
</cpix:DRMSystem>
</cpix:DRMSystemList>
<cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
</cpix:ContentKeyPeriodList>
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
</cpix:CPIX>

```

クリアでキーを含むレスポンスペイロードのライブ例

次の例は、DRMキープロバイダーからの一般的なレスポンスペイロードを示しています。

```

<cpix:CPIX xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
xmlns:speke="urn:aws:amazon:com:speke" id="abc123">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- HLS AES-128 (systemId is implementation specific) -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="81376844-
f976-481e-a84e-cc25d39b0b33">

    <cpix:URIExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWN1dGUtYXBpLnVzLXd1c3Q0tMi5hbWF6b25hd3MuY29tL0V1Z
cpix:URIExtXKey>
    <speke:KeyFormat>aWR1bnRpdHk=</speke:KeyFormat>
    <speke:KeyFormatVersions>MQ==</speke:KeyFormatVersions>
  </cpix:DRMSystem>

```

```

<!-- HLS SAMPLE-AES -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">

<cpix:URIEExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWN1dGUtYXBpLnVzLXd1c3QtMi5hbWF6b25hd3MuY29tL0VrZ
cpix:URIEExtXKey>
  <speke:KeyFormat>Y29tLmFwcGx1LnN0cmVhbWluZ2tleWRlbG12ZXJ5</speke:KeyFormat>
  <speke:KeyFormatVersions>MQ==</speke:KeyFormatVersions>
</cpix:DRMSystem>

<!-- Common encryption (Widevine) -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
  <cpix:PSSH>AAAAanBzc2gAAAAA7e
+LqXnWSs6jyCfc1R0h7QAAAEoIARIQeSIcblaNbb7Dji6sAtKZzRoNd2lkZXZpbmVfdGVzdCIfa2V5LWlk0mVTSWNibGF0Y
cpix:PSSH>
</cpix:DRMSystem>

<!-- Common encryption / MSS (Playready) -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">

<speke:ProtectionHeader>CgMAAAEAAQAAAzwAVwBSAE0ASABFAEEARABFAFIAIAB4AG0AbABuAHMAPQAIAGgAdAB0AH
+ADwAQQBMAEcASQBEAD4AQQBFAFMAQwBUAFIAPAAvAEEATABHAEKARAA
+ADwALwBQAFIATwBUAEUAQwBUAEkATgBGAE8APgA8AEsASQBEAD4ATwBXAGoAaAB0AHIAMwB1ADkAawArAHIAZABvADEASQ
+AGgAdAB0AHAA0gAvAC8ACABsAGEAeQByAGUAYQBkAHkALgBkAGkAcgB1AGMAdAB0AGEAcABzAC4AbgB1AHQALwBwAHIALw
+ADwALwBXAFIATQBIAEUAQQBEAEUAUgA+AA==</speke:ProtectionHeader>

<cpix:PSSH>AAADMHBzc2gAAAAAmgTweZhAQoarkuZb4Ihf1QAAAxAQAwAAAQABAAAYDPABXAFIATQBIAEUAQQBEAEUAUgA
+ADwASwBFAFkATABFAE4APgAxADYAPAAvAEsARQBZAEwARQBOAD4APABBAEwARwBJAEQAPgBBAEUAUwBDAFQAUgA8AC8AQ
+ADwASwBJAEQAPgBiAGgAdwBpAGUAWQAxAFcAdgBtADMARABqAGkANgBzAEEAdABLAFoAegBRAD0APQA8AC8ASwBJAEQAPg
+AGEAVABtAFAASgBWAEMAvgBaADYAcwA9ADwALwBDAEgARQBDAEsAUwBVAE0APgA8AEwAQQBFAFUUgBMAD4AaAB0AHQA
+ADwALwBEAEEAVABBAD4APAAvAFcAUgBNAEgARQBBAEQARQBSAD4A</cpix:PSSH>
  </cpix:DRMSystem>
</cpix:DRMSystemList>
<cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
</cpix:ContentKeyPeriodList>
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" />
  </cpix:ContentKeyUsageRule>

```

```
</cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

SPEKE API v1 - VOD ワークフローメソッド呼び出しの例

リクエストの構文例

以下はURL例であり、固定形式を示すものではありません。

```
POST https://speke-compatible-server/speke/v1.0/copyProtection
```

リクエストボディ

CPIX 要素。

レスポンスヘッダー

名前	型	発生	説明
Speke-User-Agent	文字列	1..1	キープロバイダーを識別する文字列
Content-Type	文字列	1..1	application/xml

レスポンスのリクエスト

HTTP CODE	ペイロード名	発生	説明
200 (Success)	CPIX	1..1	DASH-CPIX ペイロードレスポンス
4XX (Client error)	クライアントエラーメッセージ'	1..1	クライアントエラーの説明
5XX (Server error)	サーバーエラーメッセージ	1..1	サーバーエラーの説明

Note

このセクションの例には、コンテンツキーの暗号化は含まれていません。コンテンツキーの暗号化を追加する方法については、[コンテンツキーの暗号化](#)を参照してください。

VOD クリアのキーを使用したリクエストペイロードの例

次の例は、エンクリプタからDRMキープロバイダーへの基本的なVODリクエストペイロードを示しています。

```
<cpix:CPIX id="abc123" xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
  xmlns:speke="urn:aws:amazon:com:speke">
  <cpix:ContentKeyList>
    <cpix:ContentKey kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  explicitIV="0Fj2IjCsPJFfMAxmQxLGPw=="></cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- HLS AES-128 (systemId is implementation specific)-->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="81376844-
  f976-481e-a84e-cc25d39b0b33">
      <cpix:URIEExtXKey></cpix:URIEExtXKey>
      <speke:KeyFormat></speke:KeyFormat>
      <speke:KeyFormatVersions></speke:KeyFormatVersions>
    </cpix:DRMSystem>

    <!-- HLS SAMPLE-AES -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
      <cpix:URIEExtXKey></cpix:URIEExtXKey>
      <speke:KeyFormat></speke:KeyFormat>
      <speke:KeyFormatVersions></speke:KeyFormatVersions>
    </cpix:DRMSystem>

    <!-- Common encryption (Widevine)-->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
      <cpix:PSSH></cpix:PSSH>
    </cpix:DRMSystem>

    <!-- Common encryption / MSS (Playready) -->
```

```

<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
  <speke:ProtectionHeader></speke:ProtectionHeader>
  <cpix:PSSH></cpix:PSSH>
</cpix:DRMSystem>
</cpix:DRMSystemList>
</cpix:CPIX>

```

VOD クリアのキーを使用したレスポンスペイロードの例

次の例は、DRMキープロバイダーからの基本的なVODレスポンスペイロードを示しています。

```

<cpix:CPIX xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
xmlns:speke="urn:aws:amazon:com:speke" id="abc123">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFFMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- HLS AES-128 (systemId is implementation specific) -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="81376844-
f976-481e-a84e-cc25d39b0b33">

      <cpix:URIEExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZW1dGUtYXBpLnVzLXd1c3QtMi5hbWFF6b25hd3MuY29tL0VrZ
cpix:URIEExtXKey>
      <speke:KeyFormat>aWR1bnRpdHk=</speke:KeyFormat>
      <speke:KeyFormatVersions>MQ==</speke:KeyFormatVersions>
    </cpix:DRMSystem>

    <!-- HLS SAMPLE-AES -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">

      <cpix:URIEExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZW1dGUtYXBpLnVzLXd1c3QtMi5hbWFF6b25hd3MuY29tL0VrZ
cpix:URIEExtXKey>
      <speke:KeyFormat>Y29tLmFwcGx1LnN0cmVhbWluZ2tleWR1bG12ZXJ5</speke:KeyFormat>
      <speke:KeyFormatVersions>MQ==</speke:KeyFormatVersions>
    </cpix:DRMSystem>
  </cpix:DRMSystemList>
</cpix:CPIX>

```

```

</cpix:DRMSystem>

<!-- Common encryption (Widevine) -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
  <cpix:PSSH>AAAAanBzc2gAAAAA7e
+LqXnWSs6jyCfc1R0h7QAAAEoIARIQeSIcblaNbb7Dji6sAtKZzRoNd2lkZXZpbmVfdGVzdCIfa2V5LWlk0mVTSWNibGF0Y
cpix:PSSH>
</cpix:DRMSystem>

<!-- Common encryption / MSS (Playready) -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">

<speke:ProtectionHeader>CgMAAAEAAQAAAzwAVwBSAE0ASABFAEEARABFAFIATIB4AG0AbABuAHMAPQaiAGgAdAB0AH
+ADwAQQBMAEAcASQBEAD4AQQBFMAQwBUAFIAPAAvAEeATABHAEkARAA
+ADwALwBQAFIATwBUAEUAQwBUAEkATgBGAE8APgA8AEsASQBEAD4ATwBXAGoAaAB0AHIAMwB1ADkAawArAHIAZABvADEASQ
+AGgAdAB0AHAA0gAvAC8ACABsAGEAeQByAGUAYQBkAHkALgBkAGkAcgBlAGMAdAB0AGEAcABzAC4AbgBlAHQALwBwAHIALw
+ADwALwBXAFIATQBIAEUAQQBEAEUAUgA+AA==</speke:ProtectionHeader>

<cpix:PSSH>AAADMHBzc2gAAAAAmgTweZhAQoarkuZb4Ihf1QAAAxAQAwAAAQABAAYDPABXAFIATQBIAEUAQQBEAEUAUgA
+ADwASwBFAFKATABFAE4APgAxADYAPAAvAEsARQBZAEwARQB0AD4APABBAEwARwBJAEQAPgBBAEUAUwBDAFQAUGA8AC8AQQ
+ADwASwBJAEQAPgBiAGgAdwBpAGUAWQAxAFcAdgBtADMARABqAGkAngBzAEEAdABLAFOaegBRAD0APQA8AC8ASwBJAEQAPg
+AGEAVABtAFAASgBWAEMAVgBaADYAcwA9ADwALwBDAEgARQBDAEsAUwBVAE0APgA8AEwAQQBFAFUUAUGBMAD4AaAB0AHQAcA
+ADwALwBEAEeAVABBAD4APAAvAFcAUgBNAEgARQBBAEQARQBSAD4A</cpix:PSSH>
  </cpix:DRMSystem>
</cpix:DRMSystemList>
</cpix:CPIX>

```

SPEKE API v1 - コンテンツキーの暗号化

オプションで、コンテンツキーの暗号化をSPEKE実装に追加できます。コンテンツキーの暗号化は、コンテンツ自体の暗号化に加えて、転送用のコンテンツキーを暗号化することで、完全な end-to-end 保護を保証します。キープロバイダーにこれを実装していない場合は、トランスポートレイヤーの暗号化と強力な認証をセキュリティに使用することになります。

AWS クラウドで実行されているエンクリプタにコンテンツキー暗号化を使用するには、証明書を AWS Certificate Manager にインポートし、結果の証明書ARNsを暗号化アクティビティに使用します。エンクリプタは、証明書ARNsとACMサービスを使用して、暗号化されたコンテンツキーを DRMキープロバイダーに提供します。

制限事項

SPEKE は、以下の制限がある DASH-IF CPIX仕様で指定されているコンテンツキーの暗号化をサポートします。

- SPEKE は、リクエストまたはレスポンスペイロードのデジタル署名検証 (XMLDSIG) をサポートしていません。
- SPEKE には 2048 RSAベースの証明書が必要です。

これらの制限は、[DASH「-IF 仕様のカスタマイズと制約」](#)にも記載されています。

コンテンツキーの暗号化の実装

コンテンツキーの暗号化を提供するには、DRMキープロバイダーの実装に以下を含めます。

- リクエストペイロードとレスポンスペイロードで要素 `<cpix:DeliveryDataList>` を処理します。
- レスポンスペイロードの `<cpix:ContentKeyList>` に暗号化された値を入力します。

これらの要素の詳細については、[DASH「-IF 2.0 仕様CPIX」](#)を参照してください。

レスポンスペイロードのコンテンツキー暗号化要素の例 `<cpix:DeliveryDataList>`

次の例は、追加された `<cpix:DeliveryDataList>` 要素を太字で示しています。

```
<?xml version="1.0" encoding="UTF-8"?>
<cpix:CPIX id="example-test-doc-encryption"
  xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
  xmlns:speke="urn:aws:amazon:com:speke">
  <cpix:DeliveryDataList>
    <cpix:DeliveryData id="<ORIGIN SERVER ID>">
      <cpix:DeliveryKey>
        <ds:X509Data>
          <ds:X509Certificate><X.509 CERTIFICATE, BASE-64 ENCODED></
ds:X509Certificate>
        </ds:X509Data>
      </cpix:DeliveryKey>
    </cpix:DeliveryData>
  </cpix:DeliveryDataList>
  <cpix:ContentKeyList>
    ...
```

```

</cpix:ContentKeyList>
</cpix:CPIX>

```

レスポンスペイロードのコンテンツキー暗号化要素の例 <cpix:DeliveryDataList>

次の例は、追加された <cpix:DeliveryDataList> 要素を太字で示しています。

```

<cpix:CPIX xmlns:cpix="urn:dashif:org:cpix"
  xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
  xmlns:speke="urn:aws:amazon:com:speke" id="hls_test_001">
  <cpix:DeliveryDataList>
    <cpix:DeliveryData id="<ORIGIN SERVER ID>">
      <cpix:DeliveryKey>
        <ds:X509Data>
          <ds:X509Certificate><X.509 CERTIFICATE, BASE-64 ENCODED></
ds:X509Certificate>
          </ds:X509Data>
        </cpix:DeliveryKey>
        <cpix:DocumentKey Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc">
          <cpix:Data>
            <pskc:Secret>
              <pskc:EncryptedValue>
                <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#rsa-oaep-mgf1p" />
                <enc:CipherData>
                  <enc:CipherValue><RSA CIPHER VALUE></enc:CipherValue>
                </enc:CipherData>
              </pskc:EncryptedValue>
              <pskc:ValueMAC>qnei/5TsfUwDu+8bhsZrLjDRDngvmnUZD2eva7SfXWw=</
pskc:ValueMAC>
            </pskc:Secret>
          </cpix:Data>
        </cpix:DocumentKey>
        <cpix:MACMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#hmac-
sha512">
          <cpix:Key>
            <pskc:EncryptedValue>
              <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#rsa-oaep-mgf1p" />
              <enc:CipherData>
                <enc:CipherValue><RSA CIPHER VALUE></enc:CipherValue>
              </enc:CipherData>
            </pskc:EncryptedValue>
          </cpix:Key>
        </cpix:MACMethod>
      </cpix:DeliveryData>
    </cpix:DeliveryDataList>
  </cpix:CPIX>

```

```

        <pskc:ValueMAC>DGqdpHUfFKxds09+EWrPjtdTCVfjPLwwtzEcFC/j0xY=</
pskc:ValueMAC>
        </cpix:Key>
    </cpix:MACMethod>
</cpix:DeliveryData>
</cpix:DeliveryDataList>
<cpix:ContentKeyList>
    ...
</cpix:ContentKeyList>
</cpix:CPIX>

```

レスポンスペイロードのコンテンツキー暗号化要素の例 <cpix:ContentKeyList>

次の例は、レスポンスペイロードの <cpix:ContentKeyList> 要素で暗号化されたコンテンツキーの処理を示しています。これは <pskc:EncryptedValue> 要素を使用します。

```

<cpix:ContentKeyList>
  <cpix:ContentKey kid="682681c8-69fa-4434-9f9f-1a7f5389ec02">
    <cpix:Data>
      <pskc:Secret>
        <pskc:EncryptedValue>
          <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#aes256-cbc" />
          <enc:CipherData>
            <enc:CipherValue>NJYebfvJ2TdMm3k6v
+rLNVYb0NoTJoTLBBdbpe8nmilEfp82SKa7MkqTn2lmQBPB</enc:CipherValue>
          </enc:CipherData>
        </pskc:EncryptedValue>
        <pskc:ValueMAC>t91W4WCebfS1GP+dh0IicMs+2+jnrAmfDa4WU6VGHC4=</
pskc:ValueMAC>
      </pskc:Secret>
    </cpix:Data>
  </cpix:ContentKey>
</cpix:ContentKeyList>

```

これに対して、以下の例は、クリアキーとして暗号化されていないコンテンツキーを持つ同様のレスポンスペイロードを示しています。これは <pskc:PlainValue> 要素を使用します。

```

<cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw=="
kid="682681c8-69fa-4434-9f9f-1a7f5389ec02">
    <cpix:Data>

```

```

    <pskc:Secret>
      <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
    </pskc:Secret>
  </cpix:Data>
</cpix:ContentKey>
</cpix:ContentKeyList>

```

SPEKE API v1 - ハートビート

リクエストの構文例

以下はURL例であり、固定形式を示すものではありません。

```
GET https://speke-compatible-server/speke/v1.0/heartbeat
```

レスポンスのリクエスト

HTTP CODE	ペイロード名	発生	説明
200 (Success)	statusMessage	1..1	ステータスを説明するメッセージ

SPEKE API v1 - キー識別子の上書き

エンクリプタは、キーをローテーションするたびに新しいキー識別子 (KID) を作成します。リクエストで をDRMキープロバイダーKIDに渡します。ほとんどの場合、キープロバイダーは同じ を使用して応答しますがKID、応答KIDで に別の値を指定できます。

以下は、 KID を使用したリクエストの例です11111111-1111-1111-1111-111111111111。

```

  <cpix:CPIX id="abc123" xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
  xmlns:speke="urn:aws:amazon:com:speke">
    <cpix:ContentKeyList>
      <cpix:ContentKey kid="11111111-1111-1111-1111-111111111111"></cpix:ContentKey>
    </cpix:ContentKeyList>
    <cpix:DRMSystemList>
      <!-- Common encryption (Widevine)-->
      <cpix:DRMSystem kid="11111111-1111-1111-1111-111111111111"
      systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">

```

```

    <cpix:PSSH />
  </cpix:DRMSystem>
</cpix:DRMSystemList>
<cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
</cpix:ContentKeyPeriodList>
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="11111111-1111-1111-1111-111111111111">
    <cpix:KeyPeriodFilter
periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
</cpix:CPIX>

```

次のレスポンスは、 を KID にオーバーライドしま
す 22222222-2222-2222-2222-222222222222。

```

<cpix:CPIX xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
xmlns:speke="urn:aws:amazon:com:speke" id="abc123">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="ASgwx9pQ2/2lnDzJsUxWcQ=="
kid="22222222-2222-2222-2222-222222222222">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>p3dWaHARtL97MpT7TE916w==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <cpix:DRMSystem kid="22222222-2222-2222-2222-222222222222"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
      <cpix:PSSH>AAAAanBzc2gAAAAA7e
+LqXnWSs6jyCfc1R0h7QAAAEoIARIQeSIcblaNbb7Dji6sAtKZzRoNd2lkZXZpbmVfdGVzdCIfa2V5LWlkOmVTSWNibGF0Y
cpix:PSSH>
    </cpix:DRMSystem>
  </cpix:DRMSystemList>
  <cpix:ContentKeyPeriodList>
    <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
  </cpix:ContentKeyPeriodList>

```

```
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="22222222-2222-2222-2222-222222222222">
    <cpix:KeyPeriodFilter
periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

SPEKE API v2

これは、Secure Packager and Encoder Key Exchange (SPEKE) v2 RESTAPI用の です。この仕様を使用して、暗号化を使用するお客様にDRM著作権保護を提供します。SPEKEに準拠するには、DRMキープロバイダーがこの仕様でRESTAPI説明されている を公開する必要があります。エンクリプタはキープロバイダーをAPI呼び出します。

Note

この仕様のコード例は、あくまでも説明用です。サンプルは完全なSPEKE実装の一部ではないため、実行することはできません。

SPEKE は、いくつかの制限があり、インDASHダストリーフォーラムのコンテンツ保護情報交換形式 (DASH-IF-CPIX) データ構造定義をキー交換に使用します。DASH-IF-CPIX は、DRMプラットフォームからエンクリプタへの拡張可能なマルチDRMエクスチェンジを提供するスキーマを定義します。これにより、コンテンツの圧縮およびパッケージング時に、すべての適応ビットレートパッケージング形式のコンテンツ暗号化が可能になります。アダプティブビットレートパッケージング形式にはHLS、DASH、およびが含まれますMSS。

バージョン 2.0 以降、SPEKEは特定のCPIXバージョンに合わせて調整されています。

SPEKE 側では、これは X-Speke-VersionHTTPヘッダーを使用して適用され、CPIX側ではCPIX@version 属性を使用して適用されます。リクエストにこれらの要素がないことは、v1 SPEKE レガシーワークフローの典型的な例です。SPEKE v2 ワークフローでは、キープロバイダーは両方のバージョンパラメータをサポートしている場合にのみCPIXドキュメントを処理することが期待されます。

交換形式の詳細については、DASH 「Industry Forum [CPIX2.3 specification](#)」を参照してください。

全体として、v2.0 SPEKE は v1.0 SPEKE と比較して次の進化をもたらします。

- SPEKE XML 名前空間のすべてのタグは非推奨となり、CPIXXML名前空間内の同等のタグが優先されます。
- SPEKE:ProtectionHeader は非推奨であり、CPIX:DRMSystem.SmoothStreamingProtectionHeaderData に置き換えられます
- CPIX:URIExtXKey、SPEKE:KeyFormat、および SPEKE:KeyFormatVersions は非推奨であり、CPIX:DRMSystem.HLSSignalingData に置き換えられます
- CPIX@id は CPIX@contentId に置き換えられます
- 新しい必須CPIX属性: CPIX@version、ContentKey@commonEncryptionScheme
- 新しいオプションCPIX要素: DRMSystem.ContentProtectionData
- 複数のコンテンツキーのサポート
- SPEKE と 間のクロスバージョンメカニズム CPIX
- HTTP ヘッダーの進化: 新しいX-Speke-Versionヘッダー、Speke-User-Agentヘッダーの名前が に変更されました X-Speke-User-Agent
- ハートビートAPIの非推奨

SPEKE v1.0 仕様は変更されないため、既存の実装を変更して v1SPEKE.0 ワークフローのサポートを継続する必要はありません。

トピック

- [SPEKE API v2 - DASH-IF 仕様のカスタマイズと制約](#)
- [SPEKE API v2 - 標準ペイロードコンポーネント](#)
- [SPEKE API v2 - 暗号化契約](#)
- [SPEKE API v2 - ライブワークフローメソッド呼び出しの例](#)
- [SPEKE API v2 - VOD ワークフローメソッド呼び出しの例](#)
- [SPEKE API v2 - コンテンツキーの暗号化](#)
- [SPEKE API v2 - キー識別子の上書き](#)

SPEKE API v2 - DASH-IF 仕様のカスタマイズと制約

DASH Industry Forum [CPIX2.3 仕様](#)は、多くのユースケースとトポロジをサポートしています。SPEKE API v2.0 仕様では、APIのCPIXプロファイルと の両方を定義しますCPIX。これら 2 つの目標を達成するために、以下のカスタマイズと制約によりCPIX仕様に準拠しています。

CPIX プロファイル

- SPEKE は、エンクリプタコンシューマーのワークフローに従います。
- 暗号化されたコンテンツキーの場合、 は次の制限SPEKEを適用します。
 - SPEKE は、リクエストまたはレスポンスペイロードのデジタル署名検証 (XMLDSIG) をサポートしていません。
 - SPEKE には 2048 RSAベースの証明書が必要です。
- SPEKE は、CPIX機能のサブセットのみを活用します。
 - SPEKE は UpdateHistoryItemList の機能を省略します。リストがレスポンスに存在する場合、 はそのリストSPEKEを無視します。
 - SPEKE はルート/リーフキー機能を省略します。ContentKey@dependsOnKey 属性がレスポンスに存在する場合、 はそれSPEKEを無視します。
 - SPEKE は、BitrateFilter要素と VideoFilter@wgc 属性を省略します。これらの要素または属性がCPIXペイロードに存在する場合、 はそれSPEKEを無視します。
- SPEKE v2 と交換されるCPIXドキュメントで使用できるのは、[標準ペイロードコンポーネントページ](#)または[暗号化契約ページ](#)で「サポート済み」と参照される要素または属性のみです。
- エンクリプタによるCPIXリクエストに含まれる場合、すべての要素と属性は、キープロバイダーレスポンスで有効な値を持つ必要がありますCPIX。そうでない場合、エンクリプタは停止してエラーをスローします。
- SPEKE は、KeyPeriodFilter要素によるキーローテーションをサポートします。SPEKE は、キー期間を追跡ContentKeyPeriod@indexするために のみを使用します。
- HLS シグナリングには、複数のDRMSystem.HLSSignalingData要素を使用する必要があります。1 つはDRMSystem.HLSSignalingData@playlist属性値が「media」で、もう1 つはDRMSystem.HLSSignalingData@playlist属性値が「master」です。
- キーをリクエストするとき、エンクリプタは、ContentKey 要素にオプションの @explicitIV 属性を使用することがあります。キープロバイダーは、属性がリクエストに含まれていなくても、@explicitIV を使用して IV で応答することができます。
- エンクリプタはキー識別子 (KID) を生成しますが、これは与えられたコンテンツ ID とキー期間に対して同じです。キープロバイダーには、リクエストドキュメントに対するレスポンスとして KID が含まれます。
- エンクリプタは CPIX@contentId 属性の値を含めます。この属性に対して空の値を受け取ると、キープロバイダーは説明「欠落 CPIX@」のエラーを返す必要がありますcontentId。CPIX@contentId値はキープロバイダーによって上書きできません。

CPIX@id 値が null でない場合は、キープロバイダーによって無視されます。

- エンクリプタは CPIX@version 属性の値を含めます。この属性に空の値を受け取ると、キープロバイダーはCPIX「@version を見逃す」という説明のエラーを返します。サポートされていないバージョンのリクエストを受信する場合、キープロバイダーによって返されるエラーの説明は「サポートされていない CPIX@version」になります。

CPIX@version 値をキープロバイダーでオーバーライドすることはできません。

- エンクリプタは、リクエストされたキーごとに ContentKey@commonEncryptionScheme 属性の値を含めます。この属性に空の値を受け取ると、キープロバイダーは ContentKey「@for を見逃すcommonEncryptionScheme」という説明のエラーを返しますKIDid。

一意のCPIXドキュメントは、異なるContentKey@commonEncryptionScheme属性に対して複数の値を混在させることはできません。このような組み合わせを受け取ると、キープロバイダーは「非準拠の ContentKey@commonEncryptionScheme combination」という説明のエラーを返すものとします。

すべてのContentKey@commonEncryptionScheme値がすべてのDRMテクノロジーと互換性があるわけではありません。このような組み合わせを受け取ると、キープロバイダーは ContentKey「@commonEncryptionScheme non compatible with」という説明のエラーを返すものとしますDRMSystemid。

ContentKey@commonEncryptionScheme 値をキープロバイダーでオーバーライドすることはできません。

- CPIX レスポンス本文内の DRMSystem@PSSHおよびDRMSystem.ContentProtectionData内部XML<pssh>要素に対して異なる値を受信すると、エンクリプタは停止してエラーをスローします。

CPIX に関する API

- キープロバイダーには、X-Speke-User-AgentHTTPレスポンスヘッダーの値を含める必要があります。
- SPEKE準拠のエンクリプタはクライアントとして機能し、キープロバイダーエンドポイントにPOSTオペレーションを送信します。
- エンクリプタには、X-Speke-VersionHTTPリクエストヘッダーの値を含める必要がありますMajorVersion。リクエストで使用されるSPEKEバージョンは、v2.0 の '2.0' MinorVersionのように SPEKE として指定されます。キープロバイダーが現在のリクエストでエンクリプタが使用す

るSPEKEバージョンをサポートしていない場合、キープロバイダーは「サポートされていないSPEKEバージョン」という説明のエラーを返し、ベストエフォートベースでCPIXドキュメントを処理しようとしません。

キープロバイダーは、エンクリプタによって定義された X-Speke-Version ヘッダー値をリクエストへのレスポンスで変更できません。

- レスポンス本文でエラーを受信すると、エンクリプタはエラーをスローし、v1.0 SPEKE バージョンを使用してリクエストを再試行しません。

キープロバイダーがエラーを返さないが、必須情報を含むCPIXドキュメントを返さない場合、エンクリプタは停止してエラーをスローする必要があります。

次の表は、キープロバイダーがメッセージの本文で返す必要がある標準メッセージをまとめたものです。エラーケースのHTTPレスポンスコードは 4XX または 5XX で、200 ではありません。422 エラーコードは、SPEKE/に関連するすべてのエラーに使用できますCPIX。

エラーケース	エラーメッセージ
CPIX@contentId is 定義されていません	CPIX@ がありませんcontentId
CPIX@version が定義されていません	CPIX@version がありません
CPIX@version はサポートされていません	サポートされていない CPIX@version
ContentKey@commonEncryptionScheme is 定義されていません	ContentKey@commonEncryptionScheme for がありません KID id (は ContentKey@kid 値にid等しくなります)
1つのCPIXドキュメントで使用される複数の ContentKey@commonEncryptionScheme values	非準拠の ContentKey@commonEncryption Scheme combination
ContentKey@commonEncryptionScheme は DRMテクノロジーと互換性がありません	ContentKey@commonEncryptionScheme non compatible with DRMSystem id (は DRMSystem@systemId value にid等しい)
X-Speke-Version ヘッダー値がサポートされているSPEKEバージョンではありません	サポート対象外の SPEKE バージョン

エラーケース	エラーメッセージ
暗号化契約の形式が正しくない	Malformed encryption contract (不正な形式の暗号化契約)
暗号化契約がDRMセキュリティレベルの制約と矛盾する	リクエストされたCPIX暗号化契約はサポートされていません
暗号化契約に VideoFilter または AudioFilter 要素が含まれていない	CPIX 暗号化契約がない

SPEKE API v2 - 標準ペイロードコンポーネント

1つのSPEKEリクエストを通じて、エンクリプタは、特定のコンテンツに定義されている暗号化契約に従って、複数のパッケージ形式に必要なマンフェストシグナリングとともに、複数のコンテンツキーをリクエストできます。

これらすべての側面をカバーするために、標準CPIXドキュメントは3つの必須リストセクションと、ライブコンテンツキーローテーション用のオプションのリストセクションで構成されます。

<cpix:ContentKeyList> セクションとトップレベル <cpix:CPIX> 要素

これはライブとVODストリーミングの両方に関連する必須セクションで、エンクリプタで使用する必要があるさまざまなコンテンツキーを定義します。<cpix:ContentKeyList> 要素には1つまたは複数の <cpix:ContentKey> 子要素を含めることができます。それぞれの要素は個別のコンテンツキーについて記述します。

CPIX仕様に従って、ContentKey@commonEncryptionScheme 属性の可能な値は、ISOベースメディアファイル形式のファイル仕様 (ISO/IEC 23001-7:2016) の「共通暗号化」で定義されています。

- 「cenc」: AES-CTR フルサンプルとビデオのNALサブサンプル暗号化をモードする
- 「cbc1」: AES-CBC フルサンプルとビデオのNALサブサンプル暗号化をモードする
- 'cens': AES-CTR モードの部分的なビデオNALパターン暗号化
- 'cbcs': AES-CBC モードの部分的なビデオNALパターン暗号化

次の例は、暗号化されていない単一のコンテンツキーを持つCPIXドキュメントを示しています。

```

<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="CBCS">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
  </cpix:ContentKeyList>
  ...
</cpix:CPIX>

```

デフォルトでは、以下の例のように、コンテンツキーは暗号化されません。ただし、コンテンツキーの暗号化は、<cpix:DeliveryDataList> 要素を含めることでエンクリプタによってリクエストできます。詳細については、コンテンツキーの暗号化のセクションを参照してください。

でサポートされている要素 SPEKE	必須属性	オプションの属性	必須の子要素	オプションの子要素
<cpix:CPIX >	contentId、バージョン、xmlns:cpix、xmlns:pskc	name、xmlns:enc	1 つの <cpix:ContentKeyList >、1 つの <cpix:DRMSystemList >、1 つの <cpix:ContentKeyUsageRuleList >	1 つの <cpix:DeliveryDataList >、1 つの <cpix:ContentKeyPeriodList >
<cpix:ContentKeyList >	-	id	少なくとも 1 つの <cpix:ContentKey >	-
<cpix:ContentKey >	kid、commonEncryptionScheme、データ	id、Algorithm、explicitIV	1 つの <pskc:Secret>	-

でサポートされている要素 SPEKE	必須属性	オプションの属性	必須の子要素	オプションの子要素
<pskc:Secret>	PlainValue または Encrypted Value	値MAC	-	<enc:EncryptionMethod>、<enc:CipherData>

<cpix:DRMSystemList> セクション

これはライブとVODストリーミングの両方に関連する必須セクションで、コンテンツキーとともに活用する必要があるさまざまなDRMシステムを定義します。

次の例は、単一のDRM PlayReady DRMシステム仕様を持つシステムリストを示しています。

```
<cpix:DRMSystemList>
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
    systemId="9a04f079-9840-4286-ab92-e65be0885f95">
    <cpix:HLSSignalingData playlist="media">HicXmbZ2m[...]4==</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">HicXmbZ2m[...]jEi</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>t7WwH24FI[...]YCC</cpix:ContentProtectionData>
    <cpix:PSSH>FFFFanBzc[...]A==</cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData>s5RrJ12HL[...]UBB</
cpix:SmoothStreamingProtectionHeaderData>
  </cpix:DRMSystem>
</cpix:DRMSystemList>
```

の完全なリストについてはsystemIDs、DASH-IF DRM 識別子リポジトリの[コンテンツ保護セクション](#)を参照してください。

でサポートされている要素 SPEKE	必須属性	オプションの属性	必須の子要素	オプションの子要素
<cpix:DRMSystemList>	-	id	少なくとも1つの<cpix:DRMSystem>	-

でサポートされている要素 SPEKE	必須属性	オプションの属性	必須の子要素	オプションの子要素
<cpix:DRM System >	子、systemId	ID、名前、PSSH	-	ContentProtectionData、SmoothStreamingProtectionHeaderData、プレイリスト属性値が異なる 2 つの <cpix:HLS SignalingData> 要素

DRMSystem@PSSH は、ISOカプセルBMFF化がメディアセグメントに適用される場合は必須です。DRMSystem.ContentProtectionData 内部XML<pssh>要素は、マニフェストシグナリングの目的でのみエンクリプタによって利用されます。

DRMSystem@PSSH が存在し、内部XML<pssh>要素DRMSystem.ContentProtectionDataが含まれている場合、両方の値は同じである必要があります。

マHLSマニフェストでDRMSystemシグナリングを実行する場合は、要素<cpix:HLS SignalingData playlist="media">と <cpix:HLS SignalingData playlist="master">要素の両方をCPIX リクエストとレスポンスに含める必要があります。

<cpix:ContentKeyPeriodList> セクション

これは、ライブストリーミングにのみ関連するオプションのセクションで、コンテンツに適用される暗号化期間を定義します。

<cpix:ContentKeyPeriodList> 要素には 1 つまたは複数の <cpix:ContentKeyPeriod> 子要素を含めることができます。それぞれの要素はライブタイムラインの個別の暗号化期間について記述します。id 属性の値UUIDsの一部としてを使用することは、一般的に使用されるアプローチです。

```
<cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" index="1" /
>
```

```
</cpix:ContentKeyPeriodList>
```

でサポートされている要素 SPEKE	必須属性	オプションの属性	必須の子要素	オプションの子要素
<cpix:ContentKeyPeriodList>	-	id	少なくとも 1 つの <cpix:ContentKeyPeriod>	-
<cpix:ContentKeyPeriod>	id、index	-	-	-

暗号化期間を使用する場合は、以下のセクションに示すように、暗号化キーを CPIX ドキュメント内の暗号化期間の 1 つにアタッチする必要があります。

<cpix:ContentKeyUsageRuleList> セクション

これは、ライブと VOD ストリーミングの両方に関連する必須セクションで、さまざまなコンテンツキーがストリームセット内および暗号化期間にわたってトラックを保護する方法を定義します。

<cpix:ContentKeyUsageRuleList> 要素には、1 つまたは複数の <cpix:ContentKeyUsageRule> 子要素を含めることができます。各要素は、特定の暗号化期間中に、特定のコンテンツキーがエンクリプタによって適用されるトラックを記述します。<cpix:AudioFilter> 要素には、少なくとも 1 つの <cpix:VideoFilter> 要素または 1 つの <cpix:ContentKeyUsageRule> 要素が必要です。

次の例は、特定の暗号化期間中にすべてのオーディオトラックとビデオトラックに 1 つのコンテンツキーを適用するというルールのみを含む単純なリストを示しています。

```
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
    intendedTrackType="ALL">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:AudioFilter />
    <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

でサポートされている要素 SPEKE	必須属性	オプションの属性	必須の子要素	オプションの子要素
<cpix:ContentKeyUsageRuleList >	-	id	少なくとも 1 つの <cpix:ContentKeyUsageRule >	-
<cpix:ContentKeyUsageRule >	子、intendedTrackType	-	少なくとも 1 つの <cpix:AudioFilter> または 1 つの <cpix:VideoFilter> (*)	<cpix:KeyPeriodFilter >
<cpix:KeyPeriodFilter >	periodId	-	-	-
<cpix:AudioFilter >	-	minChannels, maxChannels	-	-
<cpix:VideoFilter >	-	minPixels、maxPixels、hdr、minFps、maxFps	-	-

(*) ストリームセット内の 1 つまたは複数のトラックを保護するために単一または複数のコンテンツキーを使用することに関する詳細な説明については、ドキュメントの[暗号化契約](#)セクションを参照してください。 _

SPEKE API v2 - 暗号化契約

暗号化契約は、トラックの特性に基づいて、どのコンテンツキーが特定のストリームセット内のどのトラックを保護しているかを定義します。

ストリームセット内の異なるトラックに複数のコンテンツキーを使用することが、必須ではないものの、業界のベストプラクティスとして推奨されています。少なくとも 2 つの異なるコンテンツキー (オーディオトラック用に 1 つとビデオトラック用に 1 つ) を使用するようになっています。1 つのコ

コンテンツキーを使用して複数のトラックを暗号化することは可能ですが、エンクリプタからキープロバイダーに送信されるCPIXドキュメントで明示的にシグナルを送信する必要があります。一般的に、エンクリプタは、必要なコンテンツキーの数と、それらがさまざまなメディアトラックの暗号化にどのように活用されるかを常に正確に記述します。

原則

暗号化契約は、CPIXドキュメントの <cpix:ContentKeyUsageRuleList> セクションにあります。このセクションでは、<cpix:ContentKeyList> セクションで定義された各コンテンツキーは、特定の <cpix:ContentKeyUsageRule> 要素に対応します。これには以下が含まれます。

- 1つ以上のサブコンポーネントを参照できる ContentKeyUsageRule@intendedTrackType 属性。複数のサブコンポーネントが使用されている場合は、「+」記号で区切られます。ContentKeyUsageRule@intendedTrackType の値は暗号化契約では一意であり、複数の ContentKeyUsageRule 要素で使用することはできません。
- 1つまたは複数の <cpix:AudioFilter> または <cpix:VideoFilter> 子要素 (ContentKeyUsageRule@intendedTrackType 属性の値に応じます)。

この関係を規定するルールは次のとおりです。

- ストリームセットのすべてのオーディオトラックとビデオトラックを一意的コンテンツキーで保護する必要がある場合は、文字列 'ALL' を ContentKeyUsageRule@intendedTrackType 属性値として使用する必要があります。例 1 は、このようなユースケースを示しています。この状況では、属性を持たない <cpix:AudioFilter /> 子属性と <cpix:VideoFilter /> 子属性の両方を含める必要があります。<cpix:AudioFilter> 要素や <cpix:VideoFilter> 要素のその他の組み合わせは、この特定のコンテキストでは無効です。
- それ以外のすべてのユースケースでは、ContentKeyUsageRule@intendedTrackType 属性の値は自由に定義でき、<cpix:AudioFilter /> 子要素と <cpix:VideoFilter /> 子要素の数は、「+」記号で集計されたサブコンポーネントの数に対応する必要があります。例 2/3/4/5/6/7/9/10 は、ContentKeyUsageRule@intendedTrackType 属性の値に単一のサブコンポーネントが存在する場合のこの要件を示しています。例 8 は、複数のサブコンポーネントが使用される場合を示しています。ここで、ContentKeyUsageRule@intendedTrackType="SD+HD" は異なる属性値を持つ 2 つの別個の <cpix:VideoFilter> 子要素によって記述され、ContentKeyUsageRule@intendedTrackType="HDR+HFR+UHD" は異なる属性値を持つ 3 つの別個の <cpix:VideoFilter> 子要素によって記述されています。

フィルター

CPIX は複数のフィルタリング要素と属性を定義しますが、そのサブセットのみSPEKEをサポートします。次の表では、これらの違いを要約しています。

CPIX フィルタータイプ	全体的なSPEKEサポート	でサポートされている属性をフィルタリングする SPEKE	でサポートされていないフィルター属性 SPEKE
<cpix:VideoFilter >	あり	minPixels、maxPixels、hdr、minFps、maxFps (オプションの属性)	wcg
<cpix:AudioFilter >	あり	minChannels、maxChannels (オプションの属性)	
<cpix:KeyPeriodFilter >	あり	periodId (必須属性)	
<cpix:BitrateFilter >	なし	該当なし	該当なし
<cpix:LabelFilter >	なし	該当なし	該当なし

のCPIX仕様に従って VideoFilter、〔minPixels, maxPixels〕は両方のディメンションのすべての包含範囲であり、〔minFps, maxFps〕は maxFps ディメンションのみの包含範囲です。AudioFilterの場合、〔minChannels, maxChannels〕は両方のディメンションに含まれる範囲です。

問題のある状況

暗号化契約で提供される情報が、部分的、あいまい、または誤りである状況があります。このような場合、エンクリプタとキープロバイダーが適切に動作し、コンテンツが適切に保護されていることを保証することが重要です。次の表に、このような状況での推奨される動作を示します。

状況	エンクリプタの動作	キープロバイダーの動作
ストリームセット内の1つまたは複数のトラックにルール	エンクリプタは (CPIXペイロードの外部で) 設定を確認し、関連するトラックが暗号	該当なし: キープロバイダーはストリームセット構造を把握していません。

状況	エンクリプタの動作	キープロバイダーの動作
が適用されない (以下の例 3 を参照)	化を必要としないことを確認する必要があります。想定と異なる場合、エンクリプタはエラーをスローして、処理を停止する必要があります。	
複数のルールが重複し、特定のトラックを暗号化するために複数のコンテンツキーが提案される	エンクリプタは、最後に ContentKeyUsageRule 正常に評価された をドキュメントの順序で適用する必要があります。	該当なし: キープロバイダーはストリームセット構造を把握していません。
暗号化契約は 1 回の SPEKE リクエスト/レスポンスサイクルで変更されます。	キープロバイダーは暗号化契約を定義する役割を負わないため、エンクリプタは例外を発生させ、処理を停止します。	この状況が最初に発生しないように、キープロバイダーは SPEKE リクエストの CPIX ペイロードで受信した暗号化契約を変更しないでください。
不正な形式の暗号化契約: intendedTrackType/フィルター基数制約例外、サポートされていないフィルターまたは属性	エンクリプタは例外を発生させ、処理を停止し、SPEKE リクエストをキープロバイダーに送信しないものとします。これは、コンテンツ保護が誤って行われるか、一部のトラックが保護されない可能性が高いためです。	キープロバイダーは例外を発生させ、「Malformed encryption contract」(不正な形式の暗号化契約) エラーを返します。
暗号化契約は整いましたが、DRM セキュリティレベルの制約に違反しています。例えば、オーディオトラックと UHD ビデオトラックの両方を保護するために単一のコンテンツキーがリクエストされています。	エンクリプタが DRM セキュリティレベルの制約を把握している場合、コンテンツ保護が誤って行われる可能性が高いため、例外を発生させ、処理を停止し、キープロバイダーに SPEKE リクエストを送信しないでください。	キープロバイダーは例外を発生させ、「リクエストされた CPIX 暗号化契約がサポートされていない」エラーを返します。

状況	エンクリプタの動作	キープロバイダーの動作
暗号化契約がない	エンクリプタは、VideoFilter または AudioFilter 要素を含まない CPIX ドキュメントを送信しません。	キープロバイダーは例外を発生させ、CPIX 「暗号化契約の欠落」 エラーを返します。

暗号化契約の例

例 1: すべてのオーディオトラックとビデオトラックに 1 つのコンテンツキー

```
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
    intendedTrackType="ALL">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:AudioFilter />
    <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

例 2: すべてのビデオトラックに 1 つのコンテンツキー、すべてのオーディオトラックに 1 つのコンテンツキー

```
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
    intendedTrackType="VIDEO">
    <cpix:KeyPeriodFilter
      periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
    intendedTrackType="AUDIO">
    <cpix:KeyPeriodFilter
      periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:AudioFilter />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

例 3: すべてのオーディオトラックと暗号化されていないビデオトラックに 1 つのコンテンツキー

```
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  intendedTrackType="VIDEO">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

例 4: 異なるビデオトラック (SD/HD) に複数のコンテンツキー、すべてのオーディオトラックに 1 つのコンテンツキー

```
<cpix:ContentKeyUsageRuleList>
  <!-- Rule for SD video tracks (up to 1024x576) -->
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  intendedTrackType="SD">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter maxPixels="589824" />
  </cpix:ContentKeyUsageRule>
  <!-- Rule for HD video tracks (more than 1024x576) -->
  <cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
  intendedTrackType="HD">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter minPixels="589825" />
  </cpix:ContentKeyUsageRule>
  <!-- Rule for all audio tracks -->
  <cpix:ContentKeyUsageRule kid="53abda2-f210-43cb-bc90-f18f9a890a02"
  intendedTrackType="AUDIO">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:AudioFilter />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

例 5: 異なるビデオトラック (SD/HD/UHD) に複数のコンテンツキー、すべてのオーディオトラックに 1 つのコンテンツキー

```
<cpix:ContentKeyUsageRuleList>
  <!-- Rule for SD video tracks (up to 1024x576) -->
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  intendedTrackType="SD">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter maxPixels="589824" />
  </cpix:ContentKeyUsageRule>
```

```
<!-- Rule for HD video tracks (more than 1024x576, up to 1920x1080) -->
<cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
intendedTrackType="HD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="589825" maxPixels="2073600" />
</cpix:ContentKeyUsageRule>
<!-- Rule for UHD video tracks (more than 1920x1080) -->
<cpix:ContentKeyUsageRule kid="75c6fa78-8b5d-6d75-9653-26f41b78d1a3"
intendedTrackType="UHD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="2073601" />
</cpix:ContentKeyUsageRule>
<!-- Rule for all audio tracks -->
<cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

例 6: 異なるビデオトラック (SD/HD/UHD1/UHD2) に複数のコンテンツキー、すべてのオーディオトラックに 1 つのコンテンツキー

```
<cpix:ContentKeyUsageRuleList>
<!-- Rule for SD video tracks (up to 1024x576) -->
<cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="SD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter maxPixels="589824" />
</cpix:ContentKeyUsageRule>
<!-- Rule for HD video tracks (more than 1024x576, up to 1920x1080) -->
<cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
intendedTrackType="HD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="589825" maxPixels="2073600" />
</cpix:ContentKeyUsageRule>
<!-- Rule for UHD1 video tracks (more than 1920x1080, up to 4096x2160) -->
<cpix:ContentKeyUsageRule kid="75c6fa78-8b5d-6d75-9653-26f41b78d1a3"
intendedTrackType="UHD1">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="2073601" maxPixels="8847360" />
</cpix:ContentKeyUsageRule>
<!-- Rule for UHD2 video tracks (more than 4096x2160) -->
```

```
<cpix:ContentKeyUsageRule kid="63d2ec36-6b7c-9f34-4546-97d01f36f7c5"
intendedTrackType="UHD2">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="8847361" />
</cpix:ContentKeyUsageRule>
<!-- Rule for all audio tracks -->
<cpix:ContentKeyUsageRule kid="53abda2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="AUDIO0">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

例 7: 異なるビデオトラック (SD/HD1/HD2/UHD1//UHD2) に複数のコンテンツキー、すべてのオーディオトラックに 1 つのコンテンツキー

```
<cpix:ContentKeyUsageRuleList>
  <!-- Rule for SD video tracks (up to 1024x576) -->
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="SD">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter maxPixels="589824" />
  </cpix:ContentKeyUsageRule>
  <!-- Rule for HD1 video tracks (more than 1024x576, up to 1280x720) -->
  <cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
intendedTrackType="HD1">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter minPixels="589825" maxPixels="921600" />
  </cpix:ContentKeyUsageRule>
    <!-- Rule for HD2 video tracks (more than 1280x720, up to 1920x1080) -->
    <cpix:ContentKeyUsageRule kid="cda406d8-9d87-4f76-92da-31110e756176"
intendedTrackType="HD2">
      <cpix:KeyPeriodFilter
periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
      <cpix:VideoFilter minPixels="921601" maxPixels="2073600" />
    </cpix:ContentKeyUsageRule>
  <!-- Rule for UHD1 video tracks (more than 1920x1080, up to 4096x2160) -->
  <cpix:ContentKeyUsageRule kid="75c6fa78-8b5d-6d75-9653-26f41b78d1a3"
intendedTrackType="UHD1">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter minPixels="2073601" maxPixels="8847360" />
  </cpix:ContentKeyUsageRule>
  <!-- Rule for UHD2 video tracks (more than 4096x2160) -->
```

```
<cpix:ContentKeyUsageRule kid="63d2ec36-6b7c-9f34-4546-97d01f36f7c5"
intendedTrackType="UHD2">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="8847361" />
</cpix:ContentKeyUsageRule>
<!-- Rule for all audio tracks -->
<cpix:ContentKeyUsageRule kid="53abda2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

例 8: 異なるビデオトラック (複数の属性タイプに基づく) に複数のコンテンツキー、すべてのオーディオトラックに 1 つのコンテンツキー

```
<cpix:ContentKeyUsageRuleList>
  <!-- Rule for SD and HD video tracks-->
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="SD+HD">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter maxPixels="442368" maxFps="30" hdr="false"/>
    <cpix:VideoFilter minPixels="442369" maxPixels="2073600" maxFps="30" hdr="false"/>
  </cpix:ContentKeyUsageRule>
  <!-- Rule for HDR, HFR and UHD video tracks-->
  <cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
intendedTrackType="HDR+HFR+UHD">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter hdr="true" />
    <cpix:VideoFilter minFps="30" />
    <cpix:VideoFilter minPixels="20736001" />
  </cpix:ContentKeyUsageRule>
  <!-- Rule for all audio tracks-->
  <cpix:ContentKeyUsageRule kid="53abda2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="AUDIO">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:AudioFilter />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

例 9: すべてのビデオトラックに 1 つのコンテンツキー、ステレオおよびマルチチャンネルオーディオトラックに複数のコンテンツキー

```
<cpix:ContentKeyUsageRuleList>
<!-- Rule for video tracks-->
<cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="VIDEO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter />
</cpix:ContentKeyUsageRule>
<!-- Rule for stereo audio tracks-->
<cpix:ContentKeyUsageRule kid="53abda2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="STEREO_AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter maxChannels="2"/>
</cpix:ContentKeyUsageRule>
<!-- Rule for multichannel audio tracks-->
<cpix:ContentKeyUsageRule kid="7ae8e96f-309e-42c3-a510-24023d923373"
intendedTrackType="MULTICHANNEL_AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <AudioFilter minChannels="3"/>
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

例 10: すべてのビデオトラックに 1 つのコンテンツキー、ステレオおよび 2 つの種類のマルチチャンネルオーディオトラックに複数のコンテンツキー

```
<cpix:ContentKeyUsageRuleList>
<!-- Rule for video tracks-->
<cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="VIDEO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter />
</cpix:ContentKeyUsageRule>
<!-- Rule for stereo audio tracks-->
<cpix:ContentKeyUsageRule kid="53abda2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="STEREO_AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter maxChannels="2"/>
</cpix:ContentKeyUsageRule>
<!-- Rule for multichannel audio tracks (3 to 6 channels)-->
<cpix:ContentKeyUsageRule kid="7ae8e96f-309e-42c3-a510-24023d923373"
intendedTrackType="MULTICHANNEL_AUDIO_3_6">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter minChannels="3" maxChannels="6"/>
</cpix:ContentKeyUsageRule>
```

```

<!-- Rule for multichannel audio tracks (7 channels and more)-->
<cpix:ContentKeyUsageRule kid="81eb3761-55ff-4d22-a31d-94f01bbfd8ba"
intendedTrackType="MULTICHANNEL_AUDIO_7">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter minChannels="7"/>
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>

```

SPEKE API v2 - ライブワークフローメソッド呼び出しの例

リクエストの構文例

以下はURL例であり、固定形式を示すものではありません。

```
POST https://speke-compatible-server/speke/v2.0/copyProtection
```

リクエストボディ

CPIX ドキュメント。

リクエストヘッダー

名前	型	発生	説明
AWS Authorization	文字列	1..1	AWS Sigv4 を参照
X-Amz-Security-Token	文字列	1..1	AWS Sigv4 を参照
X-Amz-Date	文字列	1..1	AWS Sigv4 を参照
Content-Type	文字列	1..1	application/xml
X-Speke-Version	文字列	1..1	SPEKE API リクエストで使用されるバージョン MajorVersion。v2.0 の場合は「2.0MinorVersion」

名前	型	発生	説明
			のように SPEKE として指定されます。

レスポンスヘッダー

名前	型	発生	説明
X-Speke-User-Agent	文字列	1..1	キープロバイダーを識別する文字列
Content-Type	文字列	1..1	application/xml
X-Speke-Version	文字列	1..1	SPEKE API リクエストで使用されるバージョン MajorVersion。v2.0 の場合は「2.0MinorVersion」のように SPEKE として指定されます。

レスポンスのリクエスト

HTTP CODE	ペイロード名	発生	説明
200 (Success)	CPIX	1..1	DASH-CPIX ペイロードレスポンス
4XX (Client error)	クライアントエラーメッセージ	1..1	クライアントエラーの説明
5XX (Server error)	サーバーエラーメッセージ	1..1	サーバーエラーの説明

Note

このセクションの例には、コンテンツキーの暗号化は含まれていません。コンテンツキーの暗号化を追加する方法については、[コンテンツキーの暗号化](#)を参照してください。

クリアでキーを含むリクエストペイロードのライブ例

次の例は、エンクリプタからDRMキープロバイダーへの一般的なライブリクエストペイロードを示しています。すべてのビデオトラックに1つのコンテンツキー、すべてのオーディオトラックに1つのコンテンツキーがあります。

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="cbcs"></cpix:ContentKey>
    <cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abdba2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="cbcs"></cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- FairPlay -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
      <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
    </cpix:DRMSystem>
    <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
      <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
    </cpix:DRMSystem>
    <!-- Widevine -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
      <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
      <cpix:ContentProtectionData></cpix:ContentProtectionData>
      <cpix:PSSH></cpix:PSSH>
    </cpix:DRMSystem>
    <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
```

```
<cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
<cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
<cpix:ContentProtectionData></cpix:ContentProtectionData>
<cpix:PSSH></cpix:PSSH>
</cpix:DRMSystem>
<!-- Playready -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
  <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  <cpix:ContentProtectionData></cpix:ContentProtectionData>
  <cpix:PSSH></cpix:PSSH>
  <cpix:SmoothStreamingProtectionHeaderData></
cpix:SmoothStreamingProtectionHeaderData>
</cpix:DRMSystem>
<cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
  <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  <cpix:ContentProtectionData></cpix:ContentProtectionData>
  <cpix:PSSH></cpix:PSSH>
  <cpix:SmoothStreamingProtectionHeaderData></
cpix:SmoothStreamingProtectionHeaderData>
</cpix:DRMSystem>
</cpix:DRMSystemList>
<cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
</cpix:ContentKeyPeriodList>
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="VIDEO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter />
</cpix:ContentKeyUsageRule>
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

クリアでキーを含むレスポンスペイロードのライブ例

次の例は、DRMキープロバイダーからの一般的なレスポンスペイロードを示しています (戻り値は読みやすいように [...] で短縮されています)。

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="cbcs">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
    <cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abda2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="cbcs">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>h3toSFilyAYpfXVQ795m6x==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- FairPlay -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
      <cpix:HLSSignalingData playlist="media">aHR0cHM6L[...]WZm</cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master">Y29tLmFwc[...]XJ5</cpix:HLSSignalingData>
    </cpix:DRMSystem>
    <cpix:DRMSystem kid="53abda2-f210-43cb-bc90-f18f9a890a02"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
      <cpix:HLSSignalingData playlist="media">trBAnbMcj[...]u44</cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master">mn626PjyR[...]2fi</cpix:HLSSignalingData>
    </cpix:DRMSystem>
    <!-- Widevine -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
      <cpix:HLSSignalingData playlist="media">Ifa2V5LWl[...]nNB</cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master">oIARIQeSI[...]Nd2l</cpix:HLSSignalingData>
      <cpix:ContentProtectionData>RoNd2lkZXZ[...]Nib</cpix:ContentProtectionData>
      <cpix:PSSH>AAAAanBzc[...]A==</cpix:PSSH>
```

```

</cpix:DRMSystem>
<cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
  <cpix:HLSSignalingData playlist="media">1TznjvtzL[...]GfJ</cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master">XgzdzQH7p[...]zeX</cpix:HLSSignalingData>
  <cpix:ContentProtectionData>TdgRnuJsZ[...]wDw</cpix:ContentProtectionData>
  <cpix:PSSH>mYZbjpWdS[...]D==</cpix:PSSH>
</cpix:DRMSystem>
<!-- Playready -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
  <cpix:HLSSignalingData playlist="media">HicXmbZ2m[...]4==</cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master">GVzdCIfa2[...]Eta</cpix:HLSSignalingData>
  <cpix:ContentProtectionData>t7WwH24FI[...]YCC</cpix:ContentProtectionData>
  <cpix:PSSH>FFFFanBzc[...]A==</cpix:PSSH>
  <cpix:SmoothStreamingProtectionHeaderData>s5RrJ12HL[...]UBB</
cpix:SmoothStreamingProtectionHeaderData>
</cpix:DRMSystem>
<cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
  <cpix:HLSSignalingData playlist="media">BptGzwis2[...]Iej</cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master">3c9SXdVa0[...]MBH</cpix:HLSSignalingData>
  <cpix:ContentProtectionData>HotJCMQyc[...]GpU</cpix:ContentProtectionData>
  <cpix:PSSH>S6UD43ybN[...]f==</cpix:PSSH>
  <cpix:SmoothStreamingProtectionHeaderData>VBFUv2or0[...]JeP</
cpix:SmoothStreamingProtectionHeaderData>
</cpix:DRMSystem>
</cpix:DRMSystemList>
<cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
</cpix:ContentKeyPeriodList>
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="VIDEO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter />
</cpix:ContentKeyUsageRule>
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>

```

</cpix:CPIX>

SPEKE API v2 - VOD ワークフローメソッド呼び出しの例

リクエストの構文例

以下はURL例であり、固定形式を示すものではありません。

```
POST https://speke-compatible-server/speke/v2.0/copyProtection
```

リクエストボディ

CPIX ドキュメント。

リクエストヘッダー

名前	型	発生	説明
AWS Authorization	文字列	1..1	AWS Sigv4 を参照
X-Amz-Security-Token	文字列	1..1	AWS Sigv4 を参照
X-Amz-Date	文字列	1..1	AWS Sigv4 を参照
Content-Type	文字列	1..1	application/xml
X-Speke-Version	文字列	1..1	SPEKE API リクエストで使用されるバージョン MajorVersion。v2.0 の場合は「2.0MinorVersion」のように SPEKE として指定されます。

レスポンスヘッダー

名前	型	発生	説明
X-Speke-User-Agent	文字列	1..1	キープロバイダーを識別する文字列
Content-Type	文字列	1..1	application/xml
X-Speke-Version	文字列	1..1	SPEKE API リクエストで使用されるバージョン MajorVersion。v2.0 の場合は「2.0MinorVersion」のように SPEKE として指定されます。

レスポンスのリクエスト

HTTP CODE	ペイロード名	発生	説明
200 (Success)	CPIX	1..1	DASH-CPIX ペイロードレスポンス
4XX (Client error)	クライアントエラーメッセージ	1..1	クライアントエラーの説明
5XX (Server error)	サーバーエラーメッセージ	1..1	サーバーエラーの説明

Note

このセクションの例には、コンテンツキーの暗号化は含まれていません。コンテンツキーの暗号化を追加する方法については、[コンテンツキーの暗号化](#)を参照してください。

VOD クリアのキーを使用したリクエストペイロードの例

次の例は、エンクリプタからDRMキープロバイダーへの一般的なVODリクエストペイロードを示しています。すべてのビデオトラックに1つのコンテンツキー、すべてのオーディオトラックに1つのコンテンツキーがあります。

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="CBCS"></cpix:ContentKey>
    <cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abda2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="CBCS"></cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- FairPlay -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
      <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
    </cpix:DRMSystem>
    <cpix:DRMSystem kid="53abda2-f210-43cb-bc90-f18f9a890a02"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
      <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
    </cpix:DRMSystem>
    <!-- Widevine -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
      <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
      <cpix:ContentProtectionData></cpix:ContentProtectionData>
      <cpix:PSSH></cpix:PSSH>
    </cpix:DRMSystem>
    <cpix:DRMSystem kid="53abda2-f210-43cb-bc90-f18f9a890a02"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
      <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
      <cpix:ContentProtectionData></cpix:ContentProtectionData>
      <cpix:PSSH></cpix:PSSH>
    </cpix:DRMSystem>
    <!-- Playready -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
      <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
```

```

    <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
    <cpix:ContentProtectionData></cpix:ContentProtectionData>
    <cpix:PSSH></cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData></
cpix:SmoothStreamingProtectionHeaderData>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
    <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
    <cpix:ContentProtectionData></cpix:ContentProtectionData>
    <cpix:PSSH></cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData></
cpix:SmoothStreamingProtectionHeaderData>
  </cpix:DRMSystem>
</cpix:DRMSystemList>
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="VIDEO">
    <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="AUDIO">
    <cpix:AudioFilter />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
</cpix:CPIX>

```

VOD クリアのキーを使用したレスポンスペイロードの例

次の例は、DRMキープロバイダーからの一般的なレスポンスペイロードを示しています (読みやすいように、返された値は [...] で短縮されています)。

```

<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="CBCS">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
  </cpix:ContentKeyList>
</cpix:CPIX>

```

```

</cpix:ContentKey>
<cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abdba2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="cbcs">
  <cpix:Data>
    <pskc:Secret>
      <pskc:PlainValue>h3toSFilyAYpfXVQ795m6x==</pskc:PlainValue>
    </pskc:Secret>
  </cpix:Data>
</cpix:ContentKey>
</cpix:ContentKeyList>
<cpix:DRMSystemList>
  <!-- FairPlay -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
  <cpix:HLSSignalingData playlist="media">aHR0cHM6L[...]WZm</cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master">Y29tLmFwc[...]XJ5</cpix:HLSSignalingData>
</cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
  <cpix:HLSSignalingData playlist="media">trBANbMcyj[...]u44</cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master">mn626PjyR[...]2fi</cpix:HLSSignalingData>
</cpix:DRMSystem>
  <!-- Widevine -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
  <cpix:HLSSignalingData playlist="media">Ifa2V5LW1[...]nNB</cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master">oIARIQeSI[...]Nd21</cpix:HLSSignalingData>
  <cpix:ContentProtectionData>RoNd2lkZXZ[...]Nib</cpix:ContentProtectionData>
  <cpix:PSSH>AAAAanBzc[...]A==</cpix:PSSH>
</cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
  <cpix:HLSSignalingData playlist="media">1TznjvtzL[...]GfJ</cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master">XgzdzQH7p[...]zeX</cpix:HLSSignalingData>
  <cpix:ContentProtectionData>TdgRnuJsZ[...]wDw</cpix:ContentProtectionData>
  <cpix:PSSH>mYZbjpWdS[...]D==</cpix:PSSH>
</cpix:DRMSystem>
  <!-- Playready -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
  <cpix:HLSSignalingData playlist="media">HicXmbZ2m[...]4==</cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master">GVzdCIfa2[...]Eta</cpix:HLSSignalingData>
  <cpix:ContentProtectionData>t7WwH24FI[...]YCC</cpix:ContentProtectionData>
  <cpix:PSSH>FFFFanBzc[...]A==</cpix:PSSH>

```

```
<cpix:SmoothStreamingProtectionHeaderData>s5RrJ12HL[...]UBB</cpix:SmoothStreamingProtectionHeaderData>
</cpix:DRMSystem>
<cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
  <cpix:HLSSignalingData playlist="media">BptGzwis2[...]Iej</cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master">3c9SXdVa0[...]MBH</cpix:HLSSignalingData>
  <cpix:ContentProtectionData>HotJCMQyc[...]GpU</cpix:ContentProtectionData>
  <cpix:PSSH>S6UD43ybN[...]f==</cpix:PSSH>
  <cpix:SmoothStreamingProtectionHeaderData>VBFUv2or0[...]JeP</cpix:SmoothStreamingProtectionHeaderData>
</cpix:DRMSystem>
</cpix:DRMSystemList>
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="VIDEO">
  <cpix:VideoFilter />
</cpix:ContentKeyUsageRule>
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="AUDIO">
  <cpix:AudioFilter />
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

SPEKE API v2 - コンテンツキーの暗号化

オプションで、コンテンツキーの暗号化をSPEKE実装に追加できます。コンテンツキーの暗号化は、コンテンツ自体の暗号化に加えて、転送用のコンテンツキーを暗号化することで、完全な end-to-end 保護を保証します。キープロバイダーにこれを実装していない場合は、トランスポートレイヤーの暗号化と強力な認証をセキュリティに使用することになります。

AWS クラウドで実行されているエンクリプタにコンテンツキー暗号化を使用するには、証明書を AWS Certificate Manager にインポートし、結果の証明書ARNsを暗号化アクティビティに使用します。エンクリプタは、証明書ARNsとACMサービスを使用して、暗号化されたコンテンツキーを DRMキープロバイダーに提供します。

制限事項

SPEKE は、以下の制限がある DASH-IF CPIX仕様で指定されているコンテンツキー暗号化をサポートします。

- SPEKE は、リクエストまたはレスポンスペイロードのデジタル署名検証 (XMLDSIG) をサポートしていません。
- SPEKE には 2048 RSA ベースの証明書が必要です。

これらの制限は、[DASH 「-IF 仕様のカスタマイズと制約」](#)にも記載されています。

コンテンツキーの暗号化の実装

コンテンツキーの暗号化を提供するには、DRM キープロバイダーの実装に以下を含めます。

- リクエストペイロードとレスポンスペイロードで要素 `<cpix:DeliveryDataList>` を処理します。
- レスポンスペイロードの `<cpix:ContentKeyList>` に暗号化された値を入力します。

これらの要素の詳細については、[DASH 「-IF 2.3 仕様CPIX」](#)を参照してください。

レスポンスペイロードのコンテンツキー暗号化要素の例 `<cpix:DeliveryDataList>`

```
<cpix:CPIX contentId="abc123"
  version="2.3"
  xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
  <cpix:DeliveryDataList>
    <cpix:DeliveryData id="<ORIGIN SERVER ID>">
      <cpix:DeliveryKey>
        <ds:X509Data>
          <ds:X509Certificate><X.509 CERTIFICATE, BASE-64 ENCODED></
ds:X509Certificate>
        </ds:X509Data>
      </cpix:DeliveryKey>
    </cpix:DeliveryData>
  </cpix:DeliveryDataList>
  <cpix:ContentKeyList>
    ...
  </cpix:ContentKeyList>
</cpix:CPIX>
```

レスポンスペイロードのコンテンツキー暗号化要素の例 `<cpix:DeliveryDataList>`

```
<cpix:CPIX contentId="abc123"
  version="2.3"
```

```

xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
<cpix:DeliveryDataList>
  <cpix:DeliveryData id="<ORIGIN SERVER ID>">
    <cpix:DeliveryKey>
      <ds:X509Data>
        <ds:X509Certificate><X.509 CERTIFICATE, BASE-64 ENCODED></
ds:X509Certificate>
      </ds:X509Data>
    </cpix:DeliveryKey>
    <cpix:DocumentKey Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc">
      <cpix:Data>
        <pskc:Secret>
          <pskc:EncryptedValue>
            <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#rsa-oaep-mgf1p" />
            <enc:CipherData>
              <enc:CipherValue><RSA CIPHER VALUE></enc:CipherValue>
            </enc:CipherData>
          </pskc:EncryptedValue>
          <pskc:ValueMAC>qnei/5TsfUwDu+8bhsZrLjDRDngvmnUZD2eva7SfXWw=</
pskc:ValueMAC>
        </pskc:Secret>
      </cpix:Data>
    </cpix:DocumentKey>
    <cpix:MACMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#hmac-
sha512">
      <cpix:Key>
        <pskc:EncryptedValue>
          <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#rsa-oaep-mgf1p" />
          <enc:CipherData>
            <enc:CipherValue><RSA CIPHER VALUE></enc:CipherValue>
          </enc:CipherData>
        </pskc:EncryptedValue>
        <pskc:ValueMAC>DGqdpHUfFKxds09+EWrPjtdTCVfjPLwwtzEcFC/j0xY=</
pskc:ValueMAC>
      </cpix:Key>
    </cpix:MACMethod>
  </cpix:DeliveryData>
</cpix:DeliveryDataList>
<cpix:ContentKeyList>
  ...
</cpix:ContentKeyList>

```

```
</cpix:CPIX>
```

レスポンスペイロードのコンテンツキー暗号化要素の例 <cpix:ContentKeyList>

次の例は、レスポンスペイロードの <cpix:ContentKeyList> 要素で暗号化されたコンテンツキーの処理を示しています。これは <pskc:EncryptedValue> 要素を使用します。

```
<cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-
a20d-163a-e382420c6eff" commonEncryptionScheme="cbcs">
    <cpix:Data>
      <pskc:Secret>
        <pskc:EncryptedValue>
          <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmllenc#aes256-cbc" />
          <enc:CipherData>
            <enc:CipherValue>NJYebfvJ2TdMm3k6v
+rLNVYb0NoTJoTLBdbpe8nmilEfp82SKa7MkqTn2lmQBPB</enc:CipherValue>
          </enc:CipherData>
        </pskc:EncryptedValue>
        <pskc:ValueMAC>t9lW4WCebfS1GP+dh0IicMs+2+jnrAmfDa4WU6VGHc4=</
pskc:ValueMAC>
      </pskc:Secret>
    </cpix:Data>
  </cpix:ContentKey>
</cpix:ContentKeyList>
```

これに対して、以下の例は、クリアキーとして暗号化されていないコンテンツキーを持つ同様のレスポンスペイロードを示しています。これは <pskc:PlainValue> 要素を使用します。

```
<cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-
a20d-163a-e382420c6eff" commonEncryptionScheme="cbcs">
    <cpix:Data>
      <pskc:Secret>
        <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
      </pskc:Secret>
    </cpix:Data>
  </cpix:ContentKey>
</cpix:ContentKeyList>
```

SPEKE API v2 - キー識別子の書き

エンクリプタは、キーをローテーションするたびに新しいキー識別子 (KID) を作成します。リクエストで を DRM キープロバイダー KID に渡します。ほとんどの場合、キープロバイダーは同じ を使用して応答しますが KID、応答 KID で に別の値を指定できます。

以下は、 KID を使用したリクエストの例です 11111111-1111-1111-1111-111111111111。

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw=="
      kid="11111111-1111-1111-1111-111111111111" commonEncryptionScheme="cbcs"></
cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- Widevine -->
    <cpix:DRMSystem kid="11111111-1111-1111-1111-111111111111"
      systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
      <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
      <cpix:ContentProtectionData></cpix:ContentProtectionData>
      <cpix:PSSH></cpix:PSSH>
    </cpix:DRMSystem>
  </cpix:DRMSystemList>
  <cpix:ContentKeyPeriodList>
    <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
      index="1" />
  </cpix:ContentKeyPeriodList>
  <cpix:ContentKeyUsageRuleList>
    <cpix:ContentKeyUsageRule kid="11111111-1111-1111-1111-111111111111"
      intendedTrackType="VIDEO">
      <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
      <cpix:VideoFilter />
    </cpix:ContentKeyUsageRule>
  </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

次のレスポンスは、 を KID にオーバーライドします 22222222-2222-2222-2222-222222222222。

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw=="
kid="22222222-2222-2222-2222-222222222222" commonEncryptionScheme="cbcs">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- Widevine -->
    <cpix:DRMSystem kid="22222222-2222-2222-2222-222222222222"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
      <cpix:HLSSignalingData playlist="media">Ifa2V5LWl[...]nNB</cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master">oIARIQeSI[...]Nd2l</cpix:HLSSignalingData>
      <cpix:ContentProtectionData>RoNd2lkZXZ[...]Nib</cpix:ContentProtectionData>
      <cpix:PSSH>AAAAanBzc[...]A==</cpix:PSSH>
    </cpix:DRMSystem>
  </cpix:DRMSystemList>
  <cpix:ContentKeyPeriodList>
    <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
  </cpix:ContentKeyPeriodList>
  <cpix:ContentKeyUsageRuleList>
    <cpix:ContentKeyUsageRule kid="22222222-2222-2222-2222-222222222222"
intendedTrackType="VIDEO">
      <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
      <cpix:VideoFilter />
    </cpix:ContentKeyUsageRule>
  </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

SPEKE API 仕様のライセンス

Creative Commons Attribution-ShareAlike 4.0 国際パブリックライセンス

ライセンスされた権利 (以下に定義) を行使することにより、あなたは、このクリエイティブコモンズ帰属-ShareAlike 4.0 国際パブリックライセンス (「パブリックライセンス」) の条項に拘束されることを承諾し、同意するものとします。本パブリックライセンスが契約と解釈されるであろう範囲に

において、あなたはこれらの利用条件のあなたによる受諾と引き換えにライセンスされた権利を付与されます。そして、許諾者は、あなたに対し、それらの条項のもとでライセンス対象物を利用可能にすることから許諾者が受領する利益と引き換えに、そのような権利を付与します。

第 1 条 – 定義

- a. 「翻案物」とは、著作権およびそれに類する権利の対象となり、ライセンス対象物について許諾者が有する著作権およびそれに類する権利に基づく許諾が必要とされるような形で、翻訳され、改変され、編集され、変形され、またはその他の方法により変更されたマテリアルで、ライセンス対象物から派生したか、またはライセンス対象物に基づくものを意味します。本パブリックライセンスにおいては、ライセンス対象物が音楽作品、実演または録音物で、これらが動画と同期させられる場合には、翻案物が常に作成されることとなります。
- b. 「翻案者のライセンス」とは、翻案物に対してあなたが寄与した部分に生じる、あなたの著作権およびそれに類する権利について、本パブリックライセンスの条項に従って、あなたが適用するライセンスのことをいいます。
- c. BY-SA 互換ライセンスとは、クリエイティブコモンズによって本質的に本パブリックライセンスに相当するものとして承認された、creativecommons.org/compatiblelicenses に記載されているライセンスを意味します。
- d. 「著作権およびそれに類する権利」とは、その権利がどのように名づけられ、または分類されるかにかかわらず、著作権および/または著作権に密接に関係する類似の権利をいいます (実演、放送、録音物、およびデータベース権を含むが、これに限られません)。本パブリックライセンスにおいては、第 2 条 (b)(1) および (2) において規定される権利は、著作権およびそれに類する権利ではありません。
- e. 有効な技術的措置とは、適切な権限がない場合に、1996 年 12 月 20 日に採択された WIPO 著作権協定第 11 条に基づく義務を果たす法律および/または同様の国際協定の下で回避されない措置を意味します。
- f. 「例外および権利制限」とは、ライセンス対象物をあなたが利用する場合に適用される、フェアユース、フェアディーリングおよび/または著作権およびそれに類する権利に対するその他の例外もしくは権利制限をいいます。
- g. ライセンス要素とは、クリエイティブコモンズパブリックライセンスの名前でリストされているライセンス属性を意味します。このパブリックライセンスのライセンス要素は、帰属および `ShareAlike`。
- h. 「ライセンス対象物」とは、許諾者が本パブリックライセンスを適用した美術的または文学的著作物、データベース、またはその他のマテリアルを意味します。

- i. 「ライセンスされた権利」とは、本パブリックライセンスの条項に基づき、あなたに与えられる権利をいい、かかる権利は、あなたによるライセンス対象物の利用に適用され、かつ、許諾者がライセンスする権限を有する、全ての著作権およびそれに類する権利に限定されます。
- j. 「許諾者」とは、本パブリックライセンスのもとで権利を付与する個人または団体を意味します。
- k. 「共有」とは、複製、公開の展示、公開の上演・演奏、頒布、配布、通信または輸入のような、ライセンスされた権利に関する許諾を必要とするような手段または手法により、公衆に対しマテリアルを提供すること、および、公衆がマテリアルを利用できるようにすること (公衆の各人が、自ら独自に場所および時間を選択してマテリアルにアクセスすることができる方法を含みます) を意味します。
- l. 「データベース権」とは、データベースの法的保護に関する 1996 年 3 月 11 日の欧州議会および理事会指令 96/9/EC の結果として生じた、著作権以外の権利、(この指令が修正および/または継承された場合それらを反映したもの)、および、世界中の本質的に同等な権利を意味します。
- m. 「あなた」とは、本パブリックライセンスのもとでライセンスされた権利を行使する個人または団体をいいます。「あなたの」もそれに対応した意味となります。

第 2 条 – 範囲

a. ライセンス許諾。

- 1. 本パブリックライセンスの条項に従い、許諾者はあなたに対し、ライセンス対象物について、以下に掲げるライセンスされた権利を行使できる全世界的な、無償、再許諾不可、非排他的、かつ取消不可なライセンスを付与します:
 - A. ライセンス対象物の全部または一部を、複製および共有すること、ならびに
 - B. 翻案物を作成、複製および共有すること
- 2. 例外および権利制限 誤解を避けるために記すと、例外および権利制限があなたの利用に適用される部分については、本パブリックライセンスは適用されず、あなたは本パブリックライセンスの条項に従う必要はありません。
- 3. 期間。本パブリックライセンスの有効期間は第 6 条 (a) にて規定されます。
- 4. 媒体および形式、許可される技術的改変 許諾者は、あなたに対し、あらゆる媒体や形式 (現在知られているか、または今後作られるか否かを問いません) において、ライセンスされた権利を行使する権限、およびその行使に必要なとされる技術的な改変を行う権限を付与します。許諾者は、あなたが、ライセンスされた権利を行使するために必要とされる技術的な改変 (効果的な技術的保護手段を回避するために必要とされる技術的な改変を含みます) を禁止するいかなる権利または権限を放棄し、および/またはこれらの権利または権限を行使しないことに同意し

ます。本パブリックライセンスにおいては、本第 2 条 (a)(4) により認められる改変をするだけでは翻案物を作り出すことにはなりません。

5. ダウンストリーム (下流側) の受取人

- A. 許諾者からの申し出 – ライセンス対象物 ライセンス対象物の受取人は、許諾者から本パブリックライセンスの条項の下でライセンスされた権利を行使できるという申出を自動的に受け取ります。
- B. 許諾者からの追加の申し出 – 翻案物 翻案物の受領者は、許諾者から、あなたが申請した翻案者のライセンスの条件下で翻案物に対するライセンスされた権利を行使できるという申出を自動的に受け取ります。
- C. ダウンストリーム (下流側) への制限の禁止 あなたは、ライセンス対象物の受取人がライセンスされた権利を行使するのを制限されることになる場合には、ライセンス対象物に対して、いかなる追加条項または異なる条項も提案または課してはならず、あるいは、いかなる効果的な技術的保護手段も適用してはなりません。

- 6. 支持表明がないこと 許諾者または第 3 条 3(a)(1)(A)(i) に定められている許諾者以外のクレジット表示の対象として指定されている者が、あなたまたはライセンス対象物のあなたによる利用について、関連している、援助・支持している、あるいは正式な地位を付与している、と主張または示唆することを本パブリックライセンスは許諾しておらず、またはそのように解釈されてはなりません。

b. その他の権利。

- 1. 同一性保持の権利のような著作者人格権は、本パブリックライセンスのもとではライセンスされません。パブリシティ権、プライバシー権、および/または他の類似した人格権も同様です。ただし、可能なかぎり、許諾者は、あなたがライセンスされた権利を行使するために必要とされる範囲内で、また、その範囲内でのみ、許諾者の保持する、いかなるそのような権利を放棄し、および/または主張しないことに同意します。
- 2. 特許権および商標権は本パブリックライセンスのもとではライセンスされません。
- 3. 可能なかぎり、許諾者は、ライセンスされた権利の行使について、直接か、または任意のもしくは放棄可能な法定のもしくは強制的なライセンスに関する仕組みに基づく集中管理団体を介するかを問わず、あなたからライセンス料を得るいかなる権利も放棄します。その他一切の場合において、許諾者はそのようなライセンス料を得るいかなる権利も明確に保持します。

第 3 条 – ライセンス利用条件

ライセンスされた権利をあなたが行使するにあたっては、以下に記載された諸条件に従う必要があります。

a. 表示。

1. あなたがライセンス対象物 (変更されたものを含む) を共有する場合は以下のことを行う必要があります:

A. ライセンス対象物と共に許諾者から提供されていれば、以下のものを保持すること。

i . identification of the creator(s) of the Licensed Material and any others designated to receive attribution, in any reasonable manner requested by the Licensor (including by pseudonym if designated);

ii . a copyright notice;

iii . a notice that refers to this Public License;

iv . a notice that refers to the disclaimer of warranties;

v . a URI or hyperlink to the Licensed Material to the extent reasonably practicable;

B. ライセンス対象物を改変した場合はその旨を記し、従前の改変点についての表示も保持すること。

C. ライセンス対象物が本パブリックライセンスに基づいてライセンスされていることを示し、本パブリックライセンスのテキスト、または本パブリックライセンスへの URI またはハイパーリンクを含めること。

2. 第 3 条 (a)(1) の条件は、あなたがライセンス対象物を共有する媒体・方法・文脈に照らして、いかなる合理的な方法でも満たすことができます。例えば、必要な情報を含むリソースへの URI または のハイパーリンクを提供することで、条件を満たすことが合理的である場合があります。

3. 許諾者からリクエストされれば、あなたは第 3 条 (a)(1)(A) に掲げるいかなる情報も合理的に実施可能な範囲で削除しなければなりません。

b. ShareAlike。第 3 条 (a) の条件に加えて、あなたが作成した翻案物を共有する場合、以下の条件も適用されます。

1. あなたが申請する翻案者のライセンスは、同じライセンス要素を持つクリエイティブコモンズライセンスの本バージョン以降、または BY-SA 互換ライセンスである必要があります。

2. 適用するアダプターのライセンスのテキスト、または URI またはハイパーリンクを含める必要があります。この条件は、あなたが翻案物を共有する媒体・方法・文脈に照らして、いかなる合理的な方法でも満たすことができます。
3. あなたは、あなたが申請する翻案者のライセンスに基づいて付与された権利を行使することを制限するいかなる追加のまたは異なる条項も、翻案物に対して提案または課してはならず、あるいは、いかなる効果的な技術的保護手段も適用してはなりません。

第 4 条 – データベース権

ライセンスされた権利にデータベース権が含まれており、ライセンス対象物のあなたの利用に適用される場合:

- a. 誤解を避けるために記すと、第 2 条 (a)(1) に従い、データベースの全てまたは実質的な部分のコンテンツの抽出、再利用、複製または共有をする権利をあなたに与えます。
- b. あなたがデータベース権を持つデータベースに、あなたが、本データベースのコンテンツの全てまたは実質的な部分を含める場合、あなたがデータベース権を持つデータベース (ただし、個々のコンテンツではありません) は、本第 3 条 (b) の目的を含めて、翻案物となります。
- c. あなたは、データベースのコンテンツの全てまたは実質的な部分を共有する場合は、第 3 条 (a) の条件に従わなくてはなりません。誤解を避けるために記すと、本第 4 条は、ライセンスされた権利が他の著作権およびそれに類する権利を含む場合の本パブリックライセンス下でのあなたの義務に追加されるものであり、置き換えるものではありません。

第 5 条 – 無保証および責任制限

- a. 許諾者が別途合意しない限り、許諾者は可能な範囲において、ライセンス対象物を現状有姿のまま、現在可能な限りで提供し、明示、黙示、法令上、その他に関わらずライセンス対象物について一切の表明または保証をしません。これには、権利の帰属、商品性、特定の利用目的への適合性、権利侵害の不存在、隠れた瑕疵その他の瑕疵の不存在、正確性または誤りの存在もしくは不存在を含みますが、これに限られず、既知であるか否か、発見可能であるか否かを問いません。全部または一部の無保証が認められない場合、この無保証はあなたには適用されないこともあります。
- b. 可能な範囲において、本パブリック・ライセンスもしくはライセンス対象物の利用によって起きうる直接、特別、間接、偶発、結果的、懲罰的その他の損失、コスト、出費または損害について、例えば損失、コスト、出費、損害の可能性について許諾者が知らされていたとしても、許諾者は、あなたに対し、いかなる法理 (過失を含みますがこれに限られません) その他に基づいても責

任を負いません。全部または一部の責任制限が認められない場合、この制限はあなたには適用されないこともあります。

- c. 上記の無保証および責任制限は、可能な範囲において、全責任の完全な免責および免除に最も近いものとして解釈するものとします。

第 6 条 – 期間および終了

- a. 本パブリックライセンスは、ここでライセンスされた著作権およびそれに類する権利が有効な期間、適用されます。ただし、あなたが本パブリックライセンスに違反した場合、本パブリックライセンスに定めるあなたの権利は自動的に終了します。
- b. ライセンス対象物をあなたが利用する権利が第 6 条 (a) の事由により終了した場合でも:
1. あなたが違反を発見してから 30 日以内に違反を是正した場合に限り、違反を是正したその日に、自動的に復活します。または、
 2. 許諾者により権利の復活を明示された場合に、復活します。
- c. 誤解を避けるために記すと、本第 6 条 (b) は、許諾者が、あなたの本パブリックライセンスに関する違反に対する救済を求めるために有するであろういかなる権利にも影響を及ぼしません。
- d. 誤解を避けるために記すと、許諾者は、いつでも、別の条項の下でライセンス対象物を提供したり、ライセンス対象物の配布を停止することができます。しかし、その場合でも、本パブリックライセンスは終了しません。
- e. 第 1 条、第 5 条、第 6 条、第 7 条、第 8 条は、本パブリックライセンスが終了してもなお有効に存続します。

第 7 条 – その他の条項

- a. 許諾者は、明確に合意しない限り、あなたが通知するいかなる追加のまたは異なる条項にも拘束されません。
- b. ライセンス対象物に関する取り決め、了解事項または合意でここに言明されていない一切のものは、本パブリックライセンスの条項とは切り離され、独立したものです。

第 8 条 – 解釈

- a. 誤解を避けるために記すと、本パブリックライセンスは、本パブリックライセンスによる許諾に基づかない、ライセンス対象物のいかなる合法的な利用も縮小したり、限定したり、制限したり、条件を課したりするものではなく、またそのように解釈されてはなりません。

- b. 可能な範囲で、本パブリックライセンスのいずれかの規定が執行不能とみなされた場合には、本パブリックライセンスは、執行可能とするために必要最小限度の範囲で自動的に変更されます。もしある規定の変更が不可能な場合には、その他の条項の執行可能性に影響を与えることなく、当該規定は本パブリックライセンスから切り離されます。
- c. 本パブリックライセンスのいかなる条項も、許諾者の明確な合意なしには、放棄されることはなく、また、順守しないことに同意することはありません。
- d. 本パブリックライセンスのいかなる条項も、許諾者やあなたに適用される、あらゆる特権や免責 (司法権や当局の法的手続からの特権や免責を含む) に対する制限や放棄を構成するものではなく、またそのように解釈されるものではありません。

SPEKE パートナーとカスタマーガイドのドキュメント履歴

次の表に、SPEKEドキュメントの変更点を示します。

SPEKE v1

変更	説明	日付
サポートマトリックス: AWS パートナーサービスと製品	AWS パートナーサービスと製品でSPEKEのサポートに関する新しいセクションを追加し、Bitmovin サービスを一覧表示しました。	2023 年 1 月 13 日
DRM プラットフォームプロバイダーの更新	DRM プラットフォームプロバイダーリストにリンクと新しいパートナー情報を追加しました。	2019 年 1 月 24 日
サードパーティーのエンクリプタを含める	サードパーティーエンクリプタに対応するようにアーキテクチャと説明を更新しました。	2018 年 11 月 20 日
コンテンツキー暗号化	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、Secure Packager and Encoder Key はクリアキーの配信のみをサポートしていました。	2018 年 10 月 30 日
サポートマトリックス - AWS Elemental Live	AWS Elemental Live サポートマトリックスを追加しました。	2018 年 9 月 27 日
スタンダードペイロードコンポーネント	JSON ペイロードのメイン要素を定義するセクションを追加しました。	2018 年 9 月 27 日

変更	説明	日付
KID オーバーライド	キープロバイダーによるKID オーバーライドに関するセクションを追加しました。	2018 年 9 月 27 日
DASH-IF サイトへのリンクを修正	CPIX 仕様とシステムIDsページの IF DASH サイトへのリンクを修正しました。	2018 年 9 月 27 日
Elemental Live AWS のコピーをリリースする	Elemental AWS 製品を含めるようにSPEKEドキュメントを更新しました。	2018 年 7 月 20 日
CMAF	共通メディアアプリケーション形式 () を含むように、サービスのサポートマトリックステーブルを更新しましたCMAF。	2018 年 6 月 27 日
初回リリース	Secure Packager と Encoder Key Exchange (SPEKE) バージョン 1 の初回リリース。これは、コンテンツ暗号化者とDRMキープロバイダー間の通信の仕様です。DRM キープロバイダーは、Secure Packager と Encoder Key Exchange を公開APIして、受信キーリクエストを処理します。	2017 年 11 月 27 日

SPEKE v2

変更	説明	日付
DRM プラットフォームプロバイダーセクションとAWS	DRM プラットフォームプロバイダーリストの SPEKE v2 列に Webstream MediaConvert	2024 年 10 月 10 日

変更	説明	日付
サービスおよび製品サポート SPEKE セクションの更新	を追加し、AWS サービスと製品テーブル SPEKE のサポートの SPEKE v2 列に追加しました。	
DRM プラットフォームプロバイダーセクションの更新	DRM プラットフォームプロバイダーリストの SPEKE v2 列に新しい認定パートナーを追加しました。	2023 年 8 月 9 日
ライブおよび VOD ワークフローメソッドの呼び出し例セクションの更新	v2 Live SPEKE および VOD ワークフローメソッドの呼び出し例セクションに欠落 X-Speke-Version しているレスポンスヘッダーを追加しました。	2023 年 1 月 13 日
DRM プラットフォームプロバイダーと暗号化契約セクションの更新	DRM プラットフォームプロバイダーリストの SPEKE v2 列に新しい認定パートナーを追加しました。暗号化契約の新しい例を 2 つ追加し、関連するすべての例で SD の最大解像度を 1024x576 に変更しました。	2022 年 1 月 27 日

変更	説明	日付
初回リリース	Secure Packager と Encoder Key Exchange (SPEKE) バージョン 2.0 の初回リリース。これは、コンテンツ暗号化者とDRMキープロバイダー間の通信の仕様です。DRMキープロバイダーは、Secure Packager と Encoder Key Exchange を公開APIして、受信キーリクエストを処理します。	2021 年 9 月 7 日

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