VITEC エンドツーエンド・コンテンツ保護ソリューション 概要

VITECのIPTVおよびデジタルサイネージ・プラットフォームは、包括的かつ標準規格に準拠したコンテンツ保護ソリューションを備えています。

本ソリューションは、世界各国の主要なコンテンツプロバイダーおよびインターネットサービスプロバイダー（ISP）によって検証・承認されており、ターンキー型エンタープライズIPTVプロジェクトにおいて安心して導入できる設計となっています。

VITECのエンドツーエンドIPTVソリューションの一環として、これまでに数百件以上の導入実績を有するコンテンツ保護技術は、企業、軍事、政府機関、医療、スポーツ施設、宿泊施設など、多様な市場におけるあらゆる映像アプリケーションに必要なセキュリティと高いパフォーマンスを提供します。

概要

VITECのIPTVおよびサイネージ・プラットフォームは、コンテンツ保護に関するエンドツーエンドの包括的ソリューションを提供します。

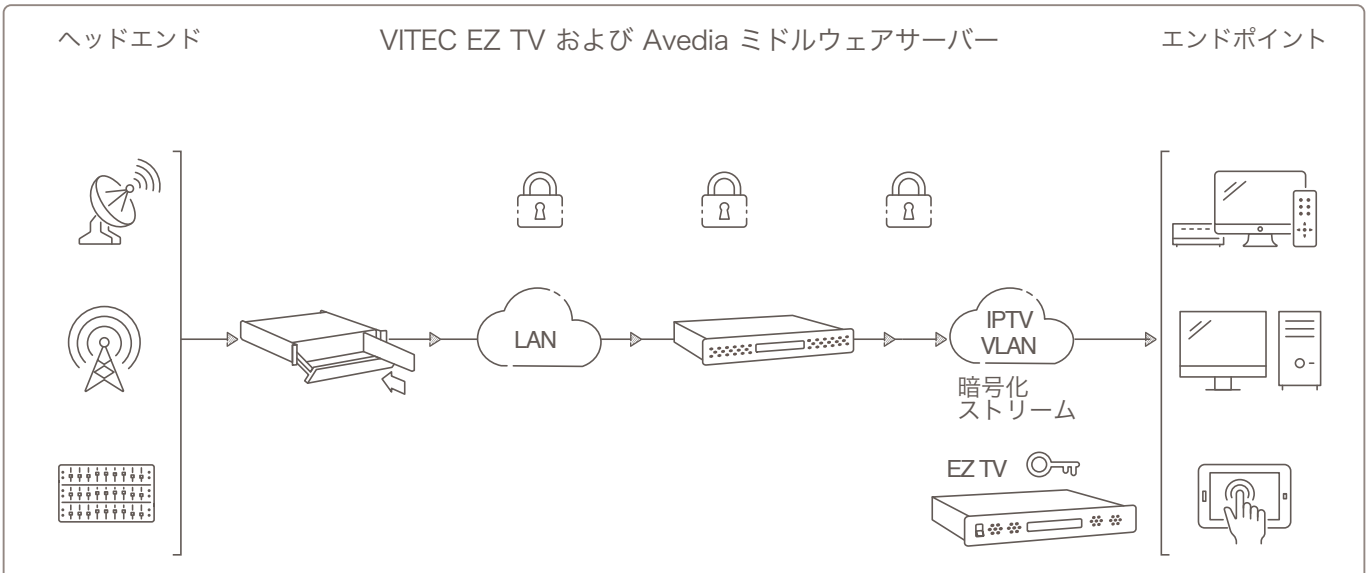
本デジタル著作権管理（DRM）アプローチは、複数の技術要素および運用手法を組み合わせることで構成されており、コンテンツそのものの保護に加え、ユーザー、再生デバイス、アクセス権限、さらには各種機能へのアクセス制御まで含めた、最高水準のセキュリティ環境を実現します。

VITECのソリューションは、Tier-1およびTier-2の放送事業者、ISP、メディア企業により、IPTVシステム内における放送コンテンツ保護用途として正式に承認されています。

さらに本ソリューションは、米国国防総省（DoD）においても、高度に機密性の高い状況把握映像および戦術軍事映像の伝送・保護用途として採用されており、極めて重要な任務を支える映像セキュリティ基盤として信頼を得ています。

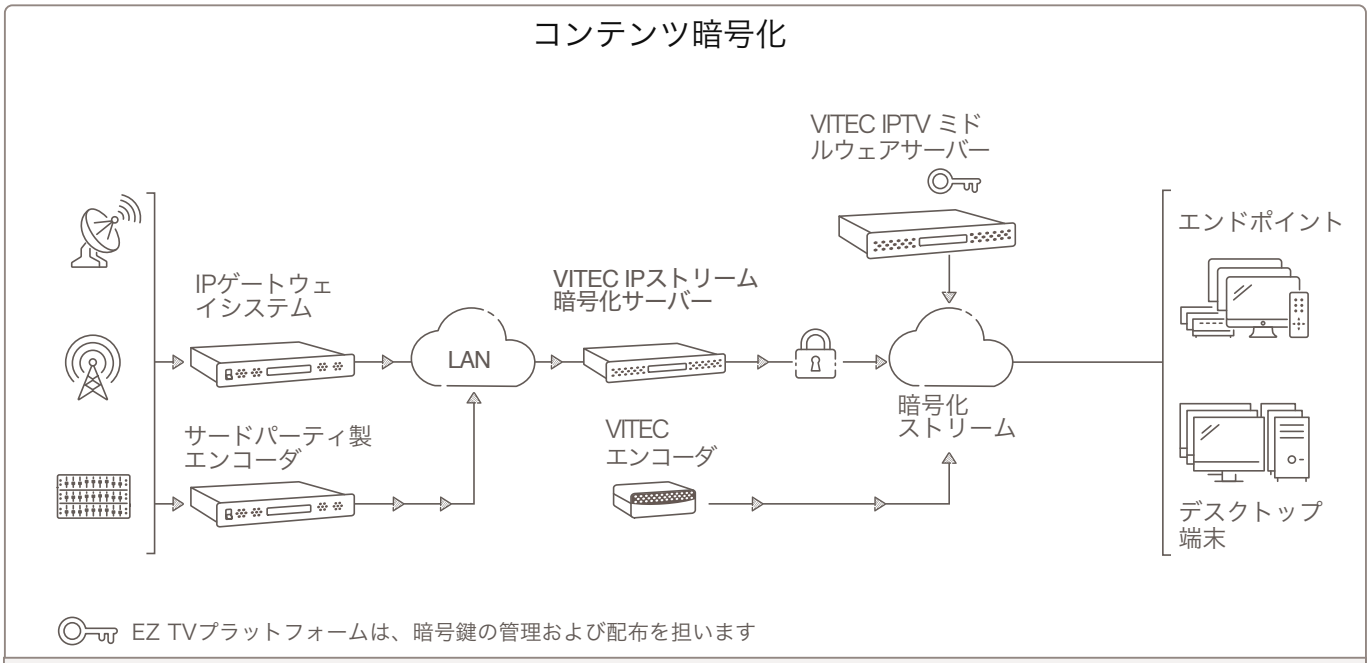
エンドツーエンド・コンテンツ保護

システム全体構成図（概要） – AES-CBC暗号化対応RFゲートウェイ統合アーキテクチャ



- 放送事業者承認のCAMを搭載したRFゲートウェイにより、受信フィードをデスクランブルし、暗号化されたマルチキャストIPTVストリームとして再配信
- ISP提供のゲートウェイが、IPTVマルチキャストコンテンツをネットワークへ配信
- ユーザー権限管理およびチャンネルラインアップの管理
- エンドポイントおよびユーザーの認証および／または検証
- 承認済みデバイスに対する暗号化／復号鍵の管理
- コンテンツへのアクセス要求
- 承認された場合にコンテンツを表示

システム全体構成図（概要） – RFゲートウェイ → UDP TSマルチキャスト出力 → VITEC暗号化サーバー



- 放送事業者承認のCAMを搭載したRFゲートウェイにより、受信フィードをデスクランブルし、暗号化されたマルチキャストIPTVストリームとして再配信
- SP提供のゲートウェイが、IPTVマルチキャストコンテンツをネットワークへ配信
- ユーザー権限およびチャンネルラインアップの管理
- エンドポイントおよびユーザーの認証ならびに検証
- 承認済みデバイスに対する暗号鍵（暗号化／復号）の管理
- コンテンツへのアクセス要求
- 承認された場合のみコンテンツを表示

- VITECのAES暗号化は、送信元とエンドポイント間で共有される鍵を使用し、MPEGトランスポートストリーム（TS）として配信されるすべての音声および映像データを暗号化します。
- 本技術は、業界標準として広く承認されているAES 128ビット CBC（Cipher Block Chaining）方式を採用し、送信元からエンドポイントまでのコンテンツを安全に暗号化します。
- ミドルウェアサーバーは、ユーザーおよびエンドポイントの承認管理に加え、暗号鍵の配布および管理を行います。
- エンドポイント到達後、コンテンツはHDCP保護されたHDMI出力を通じてディスプレイへ伝送されるため、伝送経路上でコンテンツが平文の状態で扱われることはありません。
- デバイス側のセキュリティ対策により、暗号鍵は常に暗号化された形式でのみ送信・保存されます。
- VITEC AESをVITECミドルウェアと組み合わせて使用することで、デジタル著作権管理（DRM）機能を提供します。
- 送信側マルチキャストチャネルにAES-CBC暗号化を適用できないRFゲートウェイを使用する場合、VITECのIPTV暗号化サーバーが専用の物理ネットワークおよび／または論理ネットワーク上でIPTVコンテンツを受信・中継し、リアルタイムで暗号化処理を実施します。その後、IPTVネットワーク／VLANへ配信され、ミドルウェアサーバーから鍵を付与された承認済みデバイスのみがコンテンツへアクセスし視聴できる仕組みとなっています。

送信側デバイス実装概要

RFゲートウェイは、ライブTV信号を受信・配信するために使用され、放送事業者承認のCAMを用いて信号をデスクランブルし、再暗号化した上でローカルエリアネットワーク（LAN）へストリーミング配信します。

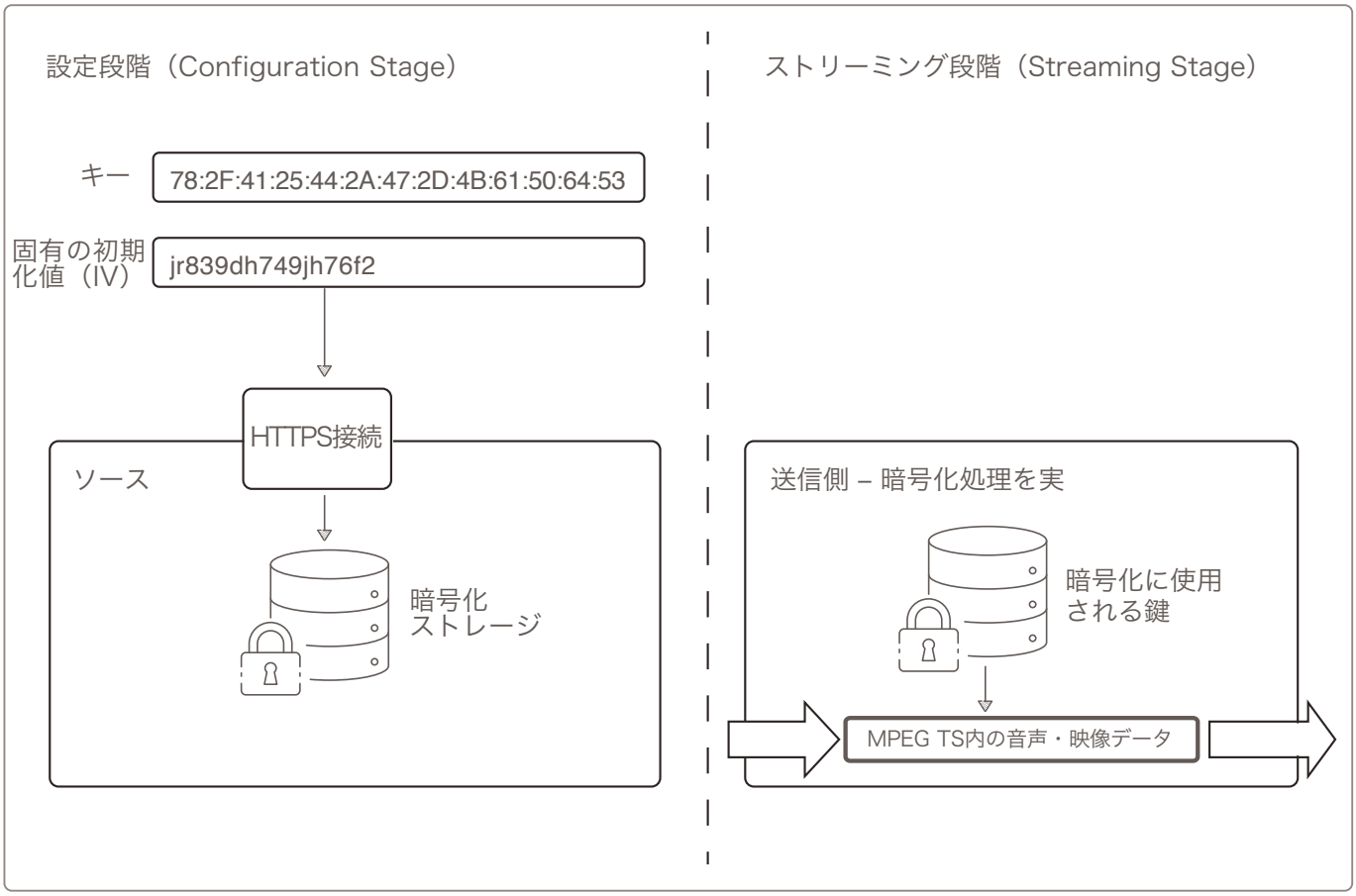
送信側デバイス（RFゲートウェイ）は、マルチキャストMPEGトランスポートストリーム（TS）形式の「チャンネル」を配信するよう構成されており、各チャンネルには個別の暗号鍵が割り当てられます。さらに、各ストリームごとに異なる初期化値（IV）を使用することで、暗号強度を一層高めることが可能です。

すべてのデスクランブル済みコンテンツは、サイトのIPTVネットワーク／VLANへ送出される前に暗号化されるため、コンテンツが平文の状態でネットワーク上を流れることはありません。

AES鍵およびIVは、安全なHTTPS接続を介して、ユーザー名／パスワードで保護された管理インターフェースから設定され、暗号化された形式で保存されます。この管理インターフェースは、コンテンツ保護機能を含むデバイスのファームウェア更新にも使用されます。

デバイスにインストールまたは更新されるすべてのファームウェアは、VITECによる署名が施されている必要があり、署名済みファームウェアのみがデバイス上で実行可能となっています。

送信側実装の構成概要は、以下の通りです。



エンドポイント・デバイス実装概要

各エンドポイントはミドルウェアサーバーを介して設定され、ミドルウェアサーバーから正しい一致鍵が提供された場合にのみ、MPEGトランスポートストリーム（TS）の音声・映像データを復号できる仕組みとなっています。

エンドポイントは起動時、およびチャンネル情報やセキュリティ情報を取得するためにサーバーへ安全な接続を開始するたびに検証が行われます。この検証には、各機器に固有に書き込まれたハードウェア固有ID（バーンインID）が使用されます。サイト内のすべての機器は、安全に難読化されたライセンスキーを用いてサーバーにより管理されており、承認されていないエンドポイントはシステムコンテンツへアクセスできません。

これらデバイスの管理はユーザーアカウント認証により保護されており、システム管理機能はすべてパスワード保護されたログインの背後に配置されています。

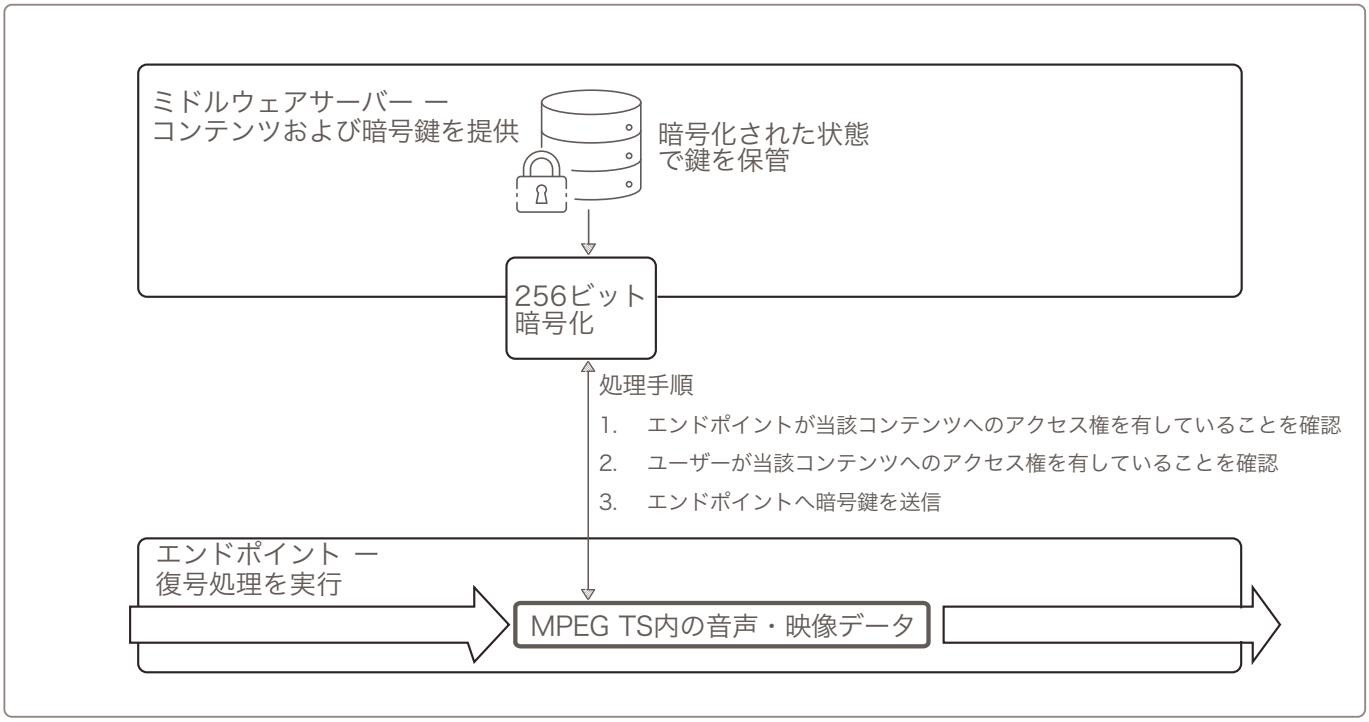
暗号鍵は暗号化された方式で安全にミドルウェアサーバーへ配信され、セッション単位の属性として保持されます。鍵は不揮発性メモリには保存されません。エンドポイントがミドルウェアサーバーに登録済みであり、かつ対象コンテンツへのアクセスが承認されたユーザー／デバイスであることが確認された場合にのみ、復号用鍵が提供されます。検証完了後、復号鍵はIPTVプラットフォームの安全な鍵交換メカニズムを通じてエンドポイントへ配信されます。

VITECのエンドポイントは、セキュア設計のハードウェアとハードニングされたリアルタイム組込みOSを基盤としています。ソフトウェアは定期的にサイバーセキュリティ検査ツールによりテストおよびスキャンが行われ、プラットフォーム全体の堅牢性を確保しています。

復号処理はエンドポイント内部で実行され、コンテンツはデコード中にのみ揮発性メモリ上に存在し、保存されることはありません。EthernetやUSBなどのデジタルインターフェース上で、コンテンツが平文状態になることはありません。

オンデバイスの管理インターフェースを使用してファームウェアの更新が可能ですが、デバイスにインストールまたは更新されるすべてのファームウェアは、VITECによる署名が施されている必要があります。署名済みファームウェアのみがデバイス上で実行可能です。

本ワークフローにおいて、鍵はエンドポイントの揮発性メモリ内に保存されるため、上書きまたはデバイス再起動時に消去されます。エンドポイントで処理されたコンテンツは当該デバイス内部でのみ利用可能であり、外部システムへ出力されることはありません。



ミドルウェア実装概要

VITECミドルウェアは、IPTVシステムにおいてエンドポイントが音声・映像コンテンツへアクセスするためのポータルとして機能します。
本ミドルウェアは、エンドポイントに対してコンテンツへのアクセスを許可または拒否する制御機能を備えています。IPTVシステム管理者によって事前に定義されたアクセス権を持たないデバイスは、コンテンツを復号するための鍵へアクセスできません。

このワークフローは、以下の技術要素を組み合わせることで、デジタル著作権管理（DRM）ソリューションを実現しています。

- 適切に構成された Active Directory または OKTA によるユーザー認証
- サーバー上に保存された暗号化ライセンスファイルに基づく エンドポイントデバイスの検証および認証（承認済みデバイスのみが認証セッションを要求可能）
- チャンネルを論理的にグループ化し、異なるアクセス権限を設定できる コンテンツグループ機能
- 実際のコンテンツペイロードに対する AES-CBC 128ビット暗号化
- 厳重に保護されたサーバーOSおよびセキュアなデータベース基盤（セキュリティ設定およびAES鍵を保存）。これらはVITECにより定期的にスキャンおよびパッチ適用が行われ、主要放送事業者および米国国防情報システム局（DISA）が定める基準を含む、最も厳格な情報保証およびサイバーセキュリティ基準への完全準拠を維持しています。
- サーバーとエンドポイント間の通信および情報ペイロードに対する AES 256ビット暗号化
- VITECの Ocaster および ChannelLink 暗号化サーバーは、ハードニングされたOSとリアルタイム暗号化エンジンを基盤とし、あらゆるUDPマルチキャストMPEG-TSに対して暗号化処理を適用可能です。また、ヘッドエンドネットワークVLANからIPTVクライアント側ネットワーク／VLANへのコンテンツ中継にも対応します。論理的および／または物理的なネットワーク分離、ならびにゼロ表示・非キャッシュのリアルタイム処理設計により、IPTVトラフィックを継続的かつ確実に保護します。

セキュリティアーキテクチャの特長

- 送信元（RFゲートウェイ）に入力されるスクランブル済みコンテンツは、放送事業者提供のCAMによりデスクランブルされた後、デバイス内部でVITEC AESにより再暗号化されます。EthernetやUSBなどのオープン／平文インターフェース上にコンテンツが露出することはありません。
- 送信元およびエンドポイント機器は、ユーザー名／パスワードにより保護され、アカウント種別に基づくアクセス制御が適用されます。エンドユーザーが利用可能なrootアカウントは存在しません。
- すべてのデバイスは、メーカーが作成し署名したファームウェアのみ実行可能です。
- 送信元、ミドルウェア、エンドポイント機器は、メーカー署名済みバイナリのみを用い、安全なHTTPS接続を通じてエンドユーザーのシステム管理者が容易に更新できます。
- 暗号化はAES-CBC方式（128ビット鍵）を採用しており、銀行、政府機関、軍事組織、放送事業者などで広く使用されている国際的な業界標準に基づいています。
- 暗号鍵が平文で保存されることはありません。
- エンドポイントは、サーバーベースのミドルウェアから鍵が提供されない限り、暗号鍵へアクセスできません。また、鍵は不揮発性メモリに保存されません。
- システム管理者は、どのユーザーおよびどのデバイスに対して特定チャンネルへのアクセスを許可するかを制御します。
- 鍵が配布される場合は、暗号化された形式で安全なトンネル内を通じて伝送されます。
- 送信元およびエンドポイント機器がコンテンツをコピーすることはありません。
- VITEC製品は、各リリースごとにセキュリティおよび情報保証（IA）上の脆弱性に対するスキャンおよび検証が実施されています。

0523

VITEC www.vitec.com

RAD 日本ラッド株式会社 映像ソリューション事業部
東京本社 〒107-6030 東京都港区赤坂 1-12-32 アーク森ビル 30 階
TEL 03-5574-7807（直通）
FAX 03-5574-7821 ／ Email info-ims@nippon-rad.co.jp
https://www.nippon-rad.co.jp