2. サーバー型放送の最新動向

2-3. サーバー型放送のアクセス制御

正会員 栗岡 辰 弥[†], 正会員 村 上 弘 規^{††}, 伊 藤 哲 規^{†††}

キーワード ■ サーバー型放送, アクセス制御, コンテンツ保護, 限定再生方式, ライセンス, コンテンツ利用条件

1 ま え が き

サーバー型放送では、前述されているような新たな視聴形態を実現するために、各コンテンツに設定された利用条件にしたがった視聴・利用の可否制御を行うアクセス制御が重要となり、その技術仕様および運用に関する規定が、従来のデジタル放送の規定に追加されている。

従来のデジタル放送では放送受信時の視聴可否しかアクセス制御できないが、サーバー型放送では、コンテンツ蓄積後の視聴・利用時、および、通信からコンテンツを取得した際の視聴・利用時にもアクセス制御を実現する。また、これらのコンテンツを視聴・利用時に必要となるライセンス（詳細は後述）は、コンテンツとは独立に放送または通信から配信できるようにすることで、通信系サービスですで行われているような多様なビジネス展開を可能としている。さらに、各コンテンツ毎に個別の許諾条件に合わせて利用条件を設定できることで、従来のデジタル放送では流せなかった新しいタイプのコンテンツを放送や通信で提供可能とし、メタデータとコンテンツを連携した新たな視聴サービスも実現可能としている。

本稿では、サーバーPで策定されたサーバー型放送運用規定を基に、サーバー型放送のアクセス制御の概要について解説する。

2 アクセス制御方式の分類

デジタル放送に関わるアクセス制御方式は、ARIB STD-B25で規定されており、受信時の制御方式である限定受信方式（CAS-R）と、再生時の制御方式である限定再生方式（CAS-P）に分類される。限定受信方式（CAS-R）は、暗号化（スクランブル）されたコンテンツを受信時に復号し、リアルタイムでコンテンツを視聴することを可能とするものである。限定再生方式（CAS-P）は、サーバー型放送受信機

図1 アクセス制御方式の分類とサービスの対象範囲

の蓄積装置に暗号化されたままの状態では蓄積したコンテンツを、再生時に復号しサービス事業者より許諾された利用条件にしたがって視聴・利用することを可能とするものである。

図1に、アクセス制御方式の分類とサーバー型放送サービスの対象範囲を示す。サーバー型放送サービスでは、アクセス制御方式として限定再生方式（CAS-P）を用い、図1に示す範囲のコンテンツをアクセス制御の対象とする。具体的には、放送でTYPE1形式またはTYPE2形式で伝送されるコンテンツ、および、通信でストリーミングまたはダウンロードで配信されるコンテンツである。なお、通信コンテンツのストリーミングには、放送と連動したAVリソースのストリーミングと、利用単位コンテンツとしてのAVリソースのストリーミング（VOD）が対象である。

3 システムリファレンスモデル

サーバー型放送におけるCASのシステムリファレンスモデルを図2に示す。次に述べる4個の論理的な構成要素と、その構成要素間における五つのインタフェースから構成される。

① CASサーバ

ライセンスの管理、ドメイン管理などを行う構成要素である。主な機能として、ライセンスの発行、関連情報の生

[†] NHK 技術局

^{††} 松下電器産業株式会社

^{†††} ソニー株式会社

"Access Control System on Broadcasting System based on Home Servers" by Tatsuya Kurioka (NHK Engineering Administration Department, Tokyo), Hiroki Murakami (Matsushita Electric Industrial Co., Ltd., Osaka) and Tetsunori Ito (Sony Corporation, Tokyo)

成・伝送、CASクライアントのドメインへの登録・削除などがある。

② CASクライアント

放送、通信経路で受信したライセンスを管理し、ライセンスに基づきコンテンツの利用を制御する構成要素である。CASクライアントは、ICカード等の耐タンパ化されたセキュリティモジュールに実装される。主な機能として、CASサーバからのライセンスの取得、ライセンスの利用条件(RMPI)に基づくコンテンツの利用可否判定、ライセンスからコンテンツの復号鍵の抽出、受信機(レンダラ)およびCASサーバの認証などがある。

③ レンダラ

暗号化されたコンテンツの再生、書き出しなどの利用を、コンテンツの復号鍵やレンダラ利用条件を保護しながら行う構成要素である。主な機能として、コンテンツのデクリプト・デスクランブル、コンテンツの再生制御(再生時間の制限、外部出力コピー制御など)、正当なセグメンテーションメタデータの識別、コンテンツのリムーバブル記録媒体・受信機内蔵の蓄積装置への書き出し、コンテンツのトランスコード・リエncrypt、CASクライアントの認証、時刻の管理などがある。

④ レジデントアプリケーション

ユーザに対するインタフェースを提供するとともに、レンダラ、および、CASクライアントの制御を行う構成要素である。主な機能として、放送および通信によるライセンスの受信、CASクライアントと連携したライセンスの管理などがある。

⑤ ライセンスの放送伝送方式/通信伝送方式

放送および通信によるライセンスの伝送仕様である。伝送されたライセンスは、⑦ レジデントアプリケーション・CASクライアント間インタフェース、または、⑧ レンダラ・CASクライアント間インタフェースにより、CASクライアントに転送される。

⑥ CASサーバ・CASクライアント間インタフェース

通信によるCASサーバとCASクライアント間のメッセージ仕様・セキュリティ仕様である。認証暗号通信路とすることで、ライセンスの不正取得などを防止する。

⑦ レジデントアプリケーション・CASクライアント間インタフェース

レジデントアプリケーションとCASクライアント間のメッセージ仕様である。

⑧ レンダラ・CASクライアント間インタフェース

レンダラとCASクライアント間のメッセージ仕様・セキュリティ仕様である。認証暗号通信路とすることで、ライセンスの不正取得などを防止する。

⑨ CASクライアント・CASクライアント間のライセンスの転送方式

CASクライアントとCASクライアント間でのライセンスの転送フォーマット仕様である。転送されたライセンスは、⑦ レジデントアプリケーション・CASクライアント間インタフェースにより、CASクライアントに転送される。

4 コンテンツの暗号化方式

4.1 放送コンテンツの暗号化方式

放送によるコンテンツの伝送形式として、TYPE1伝送とTYPE2伝送が規定されている。TYPE1伝送する際のコンテンツ暗号化をスクランブル、TYPE2伝送する際のコンテンツ(ファイル)暗号化を、エンクリプトと呼んで区別している。

TYPE1伝送のスクランブル方式には、従来のデジタル放送の限定受信方式(CAS-P)と整合性をとるため、MULTI2方式を用いる。コンテンツを復号する際に必要となるライセンスなどの関連情報は、EMMとECM(Kc伝送用ECM, ECM-Kc)の形式で伝送する。

TYPE2伝送では、コンテンツを構成する各リソース単位にエンクリプト処理を行い、エンクリプトアルゴリズムは鍵長128ビットのAES(Advanced Encryption Standard)を用いる。暗号モードはCBCモードを用いる。端数が発生した場合にはOFBモードを用いる。コンテンツを復号する際に必要となるライセンスなど関連情報は、EMMとACIの形式で伝送する。

4.2 通信コンテンツの暗号化方式

コンテンツの配信方式がストリーミング、ダウンロードともに、コンテンツとライセンスの処理としては放送のTYPE2コンテンツ(ファイル)と同様の扱いとしている。したがって、エンクリプトアルゴリズムは鍵長128ビットのAES、暗号モードはCBCモードを用いる。端数が発生した場合には、OFBモードを用いる。コンテンツを復号する際に必要となるライセンスなどの関連情報は、モジュールファイルとしてhttp(s)によるファイルダウンロードで配信する。

このように、通信系サービスで一般に呼ばれているDRMに相当する機能を含んだアクセス制御を実現している。

5 ライセンスモデル

5.1 ライセンスの定義

ライセンスとは、サービスを提供する複数リソースから構成される「利用単位コンテンツ」を利用する権利、または、ライセンスを利用する権利を示す情報である。利用条件(RMPI)と暗号コンテンツを復号するためのコンテンツ鍵、または、ライセンスを復号するためのワーク鍵が含まれる。利用条件(RMPI)とコンテンツ鍵をセットで扱う。

5.2 ライセンスの種類と鍵階層

ペーパーユースやフラット/ティアという課金形態、および、サービスの提供規模に応じた適切なライセンス伝送を実現するために、鍵階層の異なる、1階層ライセンス方式、2階層ライセンス方式の2種類を運用する。

(1) 1階層ライセンス方式

特定のCASクライアントに対して伝送する「個別ライセンス」を用いる方式。個別ライセンスには、コンテンツの利用条件(RMPI)およびコンテンツを復号する鍵が含まれる。主に、コンテンツを視聴・利用時に都度、ライセンスを取得する運用で利用される。

(2) 2階層ライセンス方式

「メインライセンス」と「サブライセンス」の2種類のライセンスを用いる方式。メインライセンスは、サブライセンスの利用を制御するためのライセンスであり、特定のCASクライアントに対して伝送される。サブライセンスは、メインライセンスのワーク鍵で暗号化され伝送されるライセンスである。サブライセンスは、対応するメインライセンスとサブライセンスの両方が有効である場合に利用可能である。放送のように、コンテンツと一緒にCASクライアントを特定せずサブライセンスを伝送し、メインライセンス

表1 運用可能なサービスとライセンスの伝送形態

コンテンツの種類	サービス形態	ライセンスモデル	ライセンス伝送方式	ライセンスの種別
TYPE1コンテンツ	フラット/ティア課金サービス	2階層ライセンス方式	放送(EMM)	ティアビット形式メインライセンス、単一サービスメインライセンス
			通信(認証暗号通信)	
			放送(Kc伝送用ECM)	ティアビット形式サブライセンス、単一サービスサブライセンス
			放送(EMM) ※サブライセンス更新時のみ	
			通信(認証暗号通信) ※サブライセンス更新時のみ	
TYPE2コンテンツ	フラット/ティア課金サービス	2階層ライセンス方式	通信(認証暗号通信)	個別ライセンス
			放送(EMM)	ティアビット形式メインライセンス、単一サービスメインライセンス
			通信(認証暗号通信)	
			放送(ACI)	ティアビット形式サブライセンス、単一サービスサブライセンス
			放送(EMM) ※サブライセンス更新時のみ	
			通信(認証暗号通信) ※サブライセンス更新時のみ	
	ペーパーユース課金サービス	1階層ライセンス方式	通信(認証暗号通信)	個別ライセンス
			通信(認証暗号通信)	個別ライセンス
通信コンテンツ(ダウンロード)	フラット/ティア課金サービス	2階層ライセンス方式	通信(認証暗号通信)	ティアビット形式メインライセンス、単一サービスメインライセンス
			通信(ACI)	
			通信(認証暗号通信) ※サブライセンス更新時のみ	ティアビット形式サブライセンス、単一サービスサブライセンス
			通信(認証暗号通信) ※サブライセンス更新時のみ	
	ペーパーユース課金サービス	1階層ライセンス方式	通信(認証暗号通信)	個別ライセンス
通信コンテンツ(AVリソースのストリーミング)	フラット/ティア課金サービス	TYPE2コンテンツのAVリソースとして取得する。 (ライセンスは、TYPE2コンテンツのライセンスを適用する)		
	ペーパーユース課金サービス			
通信コンテンツ(ストリーミング(VOD))	フラット/ティア課金サービス	1階層ライセンス方式	通信(認証暗号通信)	個別ライセンス
	ペーパーユース課金サービス

で一括制御する運用で利用される。また、サブライセンスについては、リムーバブル記録媒体などにコピーすることにより、同一ドメインに属するCASクライアント間での共有利用が可能である。

2階層ライセンス方式は、さらに、サービス毎に発行・伝送するライセンスと複数サービス一括発行・伝送するライセンスの2種類に分類できる。サービス毎に発行・伝送するライセンスを、「単一サービスメインライセンス」と「単一サービスサブライセンス」と呼び、複数サービス一括発行・伝送するライセンスを、「多サービス(ティアビット形式)メインライセンス」と「多サービス(ティアビット形式)サブライセンス」と呼ぶ。

5.3 運用可能なサービスとライセンスの伝送形態

運用可能なサービスと対応するライセンスの伝送形態を表1に示す。放送、通信の双方において柔軟なライセンス伝送と多様な課金サービスを実現している。

個別ライセンスは、認証暗号通信路で、CASサーバから特定のCASクライアントに対して伝送される。

メインライセンスは、放送ではEMMで、通信では認証暗号通信路で、CASサーバから特定のCASクライアントに対して伝送される。

サブライセンスは、放送ではKc伝送用ECM/ACIで、通信ではACIで、CASクライアントを特定せずに伝送される。ただし、サブライセンスの更新時に限り、放送ではEMM

で、通信では認証暗号通信路で、CASサーバから特定のCASクライアントに対して伝送される。

6 コンテンツの利用条件

ライセンスは、サービスに関わる複数リソースから構成される利用単位コンテンツ毎に付与することができる。アクセス制御は、コンテンツを復号する際にそのライセンスに含まれるコンテンツの利用条件(RMPI)にしたがい、コンテンツの復号鍵をCASクライアントからレンダラに出力するかどうかで、そのコンテンツの視聴・利用を制御する。その際にレンダラは、RMPIを基に生成されたレンダラ利用条件にしたがい、コンテンツの復号鍵を消費(コンテンツのデスクランブルまたはデクリプト)する。具体的なコンテンツの利用条件(RMPI)の項目を表2に示す。なお、運用の詳細については、コンテンツがTYPE1形式かTYPE2形式かなどによって異なるので運用規定を参照されたい。

(1) 再生・トリックプレイ制御

再生制御として、視聴回数、視聴期限、視聴期間を設定できる。これにより、従来の放送では流せなかったウィンドウの狭いコンテンツも放送や通信で提供可能となる。トリックプレイ制御では、その可否と早送り禁止区間が指定できる。禁止区間情報は別途TSI(Trickplay Segment Information)として記述され、利用単位コンテンツの一部

表2 コンテンツの利用条件(RMPI)項目

制御内容	利用条件(RMPI)項目	概 要
再 生	視聴回数	コンテンツの視聴可能
	視聴期限(開始日時, 終了日時)	コンテンツの視聴の視聴開始日時と視聴終了日時
	視聴期間	コンテンツ視聴開始からの視聴可能期間
トリックプレイ	トリックプレイ可否	早送り, 早戻しの可否
	早送り不可区間識別情報	早送り不可区間を示すTSI に対応するgroupId
再生時の外部出力	コピー制御形式情報	外部出力インタフェースの暗号の有無
	デジタルコピー制御情報	コピー世代を制御する情報
	出力保護ビット	高速デジタルインタフェースの保護の有無
	解像度制限ビット	映像出力信号の画質制限の有無
	アナログコピー出力制御情報	アナログ出力を制御する情報
書き出し	リムーバブル記録媒体・受信機内蔵の蓄積装置への書き出し回数	リムーバブル記録媒体・受信機内蔵の蓄積装置への書き出し回数
書き出し時の外部出力	コピー制御形式情報	外部出力インタフェースの暗号の有無
	デジタルコピー制御情報	コピー世代を制御する情報
	出力保護ビット	高速デジタルインタフェースの保護の有無
	解像度制限ビット	書き出し先リムーバブル記録媒体・受信機内蔵の蓄積装置での映像出力信号の画質制限の有無
	アナログコピー出力制御情報	書き出し先リムーバブル記録媒体・受信機内蔵の蓄積装置でのアナログ出力を制御する情報
トランスコード・リエンクリプト	トランスコード・リエンクリプト可否	トランスコードを伴うリエンクリプト可否
正当なセグメンテーションメタデータの識別	セグメンテーションメタデータ許可範囲	セグメンテーションメタデータ許可範囲
	セグメンテーションメタデータ制作者識別情報	正当なセグメンテーションメタデータの識別に用いる公開鍵証明書のシリアル番号
ドメイン	書き出し回数の転送可否	ドメイン内でのライセンスの転送時における書き出し回数の転送可否

として伝送される。

(2) 外部出力制御 (再生・書き出し)

コンテンツの暗号復号後の外部出力の扱いについて指定ができる。従来のデジタル放送の再生・録画と同等のユーザビリティを担保する運用としている。新たに想定されている、DVDに1枚焼くと100円といったサービスにも対応できるように、受信機内蔵の記録媒体に有限個の書き出しを可能とする書き出し制御ができるようになっている。なお、暗号化コンテンツをそのまま外部出力する際の制御に関しては、アクセス制御の対象にはなっていない。

(3) トランスコード・リエンクリプト制御

蓄積したコンテンツの暗号復号後にトランスコードを行い、サービス事業者が伝送したリエンクリプト鍵で再暗号化を行う指定ができる。モバイルサーバー型放送サービスなど、ハイビジョンコンテンツを標準コンテンツに変換して外部端末で視聴・利用するサービスが想定されている。

(3) セグメンテーションメタデータ制御

コンテンツを提供するサービス事業者が許諾したセグメンテーションメタデータを用いて、そのコンテンツをダイジェスト視聴することが可能となる。サービス事業者は、ダイジェスト視聴されるコンテンツ利用可能なセグメンテーションメタデータの制作者を指定できる。これにより、サービス事業者以外の第3者事業者や視聴者が制作したセグメンテーションメタデータによるコンテンツ利用を許諾することができ、コンテンツとは独立したメタデータの流通サービスが可能となる。

(4) ドメイン制御

ドメインとは、ライセンスを共有可能なCASクライアントの集合である。ドメイン制御は2階層ライセンス方式で運用され、ドメイン内の複数CASクライアント間でサブライセンスを共有可能な設定ができる。これにより、ある受信機でサービス申込みをすると、同一ドメインで設定された家庭内のすべての受信機で、コンテンツの視聴・利用を共有することが可能となる。なお、1階層ライセンス方式で提供されるコンテンツは、CASサーバ側の制御で同等な運用が可能なので、CASクライアント側での制御は想定していない。

7 む す び

サーバー型放送のアクセス制御についての概要を解説し

た。放送と通信で物理的な伝送方式の違いはあるものの、アクセス制御に関わるライセンス処理は双方で共通化した方式を実現している。これにより、放送からか通信からかコンテンツの取得経路に依らず、双方からのコンテンツを連携した視聴・利用のアクセス制御が可能である。これにより、デジタルテレビが、デジタル放送に加えてブロードバンドサービスも楽しめる健全なコンテンツ流通の共通基盤として発展し、視聴者の情報環境がより豊かに・より多様に・より柔軟になることを期待したい。

最後に、本稿で述べた運用規定策定に多大なご尽力をいただいたサーバーP、運用規定・受信機仕様策定分科会、アクセス制御方式WGの方々や、サーバー型放送CAS協議会の方々にこの場を通じて謝意を表したい。

(2006年2月15日受付)

〔文 献〕

- 1) 栗岡，柳川，福田，長尾：“サーバー型放送”，映情学誌，58，5，pp.647-650（May 2004）
- 2) 情報通信審議会 サーバー型放送システム委員会 報告書（平成14年9月30日公表），http://www.soumu.go.jp/s-news/2002/020930_4.html
- 3) ARIB STD-B25：“デジタル放送におけるアクセス制御方式”，標準規格
- 4) ARIB TR-B14：“地上デジタルテレビジョン放送運用規定”
- 5) ARIB TR-B15：“BS/広帯域CSデジタル放送運用規定”

栗岡 辰弥 1986年，東北大学大学院工学研究科電気及通信工学修士課程修了。同年，NHKに入局。1989年より，放送技術研究所にて，マルチメディア記録システム，ホームサーバ，サーバー型放送方式の研究開発および標準化に従事。2004年より，視聴者技術センター（視聴者技術計画）チーフエンジニア。1999年，研究奨励賞受賞，正会員。

村上 弘規 1981年，岡山大学工学部電子工学科卒業。同年，松下電器産業（株）に入社。以来，立体テレビシステム，アナログ放送・デジタル放送・サーバー型放送のアクセス制御方式の研究開発に従事。現在，ネットワーク開発センター主幹技師，正会員。

伊藤 哲規 1992年，（株）富士通パソコンシステムズ入社。マルチメディア系のソフトウェア開発に従事，BSデジタル放送受信システムの開発を経て，ARIBにおけるサーバー型放送方式，TV-Anytime Forumの規格化作業に参加。2000年，ソニー（株）入社後も，サーバー型放送方式の規格化全般に携わる。現在，ARIBサーバー型放送方式作業班システムTGリーダー。