5J−01

ブロードバンド時代のDRM (1)
− RightsShellによるストリーミング利用制御 −

中江 政行　岡城 純孝　細見 格　市山 俊治
NEC インターネットシステム研究所

1 はじめに

近年の急速なブロードバンド化によって，ライブ中継やVODなどのストリーミングサービスが，付加価値の高いインターネットサービスの1つとして，注目されるようになった．

一方，コンテンツサービス一般について，不正コピーなどの著作権問題が度々指摘されており，暗号技術や電子透かし技術などを利用したDRM(デジタル権利管理)システムの重要性が広く認識されつつある．

筆者らは，かねてよりコンテンツの柔軟な利用/課金制御を特徴とするDRM基盤として「RightsShell」の研究開発を進めてきた．これをストリーミングシステムに適用することで，安全性を確保しながら，様々な形態をもつストリーミングサービスが実現可能となる．

また，今後，ストリーミングサービスが普及していくにつれ，サプライサイドを含めたより高度な利用制御が求められると予想される．本稿では，特にコンテンツプロバイダの頒布権管理に着目した拡張方式を提案する．

2 ストリーミングサービスの動向

2000年末から現在にかけて見られている，xDSL網の急速な普及によって，コンサートのライブ中継などの有料ストリーミングサービスが提供されるようになった．現在，ストリーミングサービスには，ライブ中継の他，映画のVODやe-Learning等，多様なサービス形態がある．そうしたサービスは，各ISPで独立に運営されていることが多く，コンテンツおよびビジネスルールの管理は，各ISPに任されている．

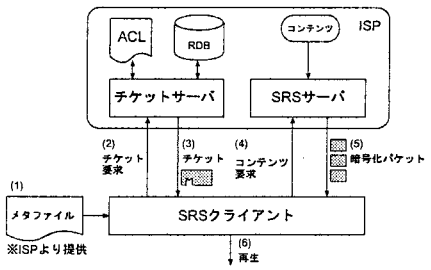

図1: ストリーミングRightsShellアーキテクチャ

DRM in the Broad-Band Era (1) − Access Control of Streaming Media with "RightsShell",
Masayuki NAKAE, Sumitaka OKAJO, Itaru HOSOMI, Shunji ICHIYAMA,
Internet System Res. Labs., NEC Corp.

今後は，各ISPが，コンテンツの企画/制作を行う事業者(CP; コンテンツプロバイダ)から高品質なコンテンツを仕入れ，配信/販売業務を行うようになると予想される．CPとISPの関係は，映画の配給会社と映画館の関係に類似することから，ストリーミングサービスにおいても，CPが持つコンテンツ配信をコントロールする権利(頒布権)を，CP自身で管理する必要が生じるものと考えられる．

3 ストリーミングRightsShell

現在のようなISP単独でのサービス形態においては，エンドユーザの視聴権を細かく制御することが課題である．

これまで筆者らは，電子書籍などのダウンロード型コンテンツに対して，柔軟な利用/課金制御を行うRightsShell[1]を研究開発してきた．今回，上記課題への解として，RightsShellをストリーミングシステムに応用した「ストリーミングRightsShell」を開発した．

3.1 基本アーキテクチャと動作

本システムの基本構成は，(1)暗号化配信機能をもつストリーミングサーバ(SRSサーバ)，(2)復号機能を持つクライアント(SRSクライアント)，(3)チケットサーバ，である(図1)．

本システムの基本動作は以下の通りである．

1. SRSクライアントにメタファイル(SRSサーバ名，チケットサーバ名，コンテンツID等)を与える．
2. SRSクライアントがチケットサーバへチケット要求を行う．
3. チケットサーバはSRSクライアントへチケットを送信する．
4. チケットを受信したSRSクライアントはSRSサーバへ配信要求を行う．
5. SRSサーバはSRSクライアントへ暗号化パケットを送出する．
6. SRSクライアントは，チケット内の復号鍵を用いて，暗号化パケットを復号しながら，コンテンツを表示する．

3.2 チケットサーバによる利用制御

RightsShellでは，チケットサーバが，コンテンツごとのビジネスルールを管理する．ビジネスルールはXML形式で文書化されており(ACLと呼ぶ)，ACLは各コン

テンツに1対1対応する形でDB管理される．ACLには，(1)コンテンツの利用主体(サブジェクト)の定義，(2)利用時にサブジェクトに求める条件(コンディション)の定義，(3)コンテンツの復号鍵，が記述される．

サブジェクトの定義は，(1)無指定(anyoneの意)，(2)サブジェクトID(ユーザIDやホストIDなど)の列挙，(3)DBの指示，などを選択できる．特に(3)については，ACSF[2]の外部リソースインターフェースを用いて，「所定のDBに格納された，所定のSQLにマッチするサブジェクトIDの全て」という定義ができ，利用者を細かく制御可能である．

また，コンディションとして，(1)課金額，(2)課金方法，(3)利用期間，(4)利用回数，などを任意に組み合わせて指定できる．これらの指定は，ACL内に静的に記述できるが，ACSMと呼んでいるプログラムモジュール[2]によって，動的に記述を生成することもできる．ACLとACSMの関係は，WWWにおけるHTMLとPHPモジュールとの関係に似ている．

チケットサーバは，サブジェクトIDとコンテンツIDとを含むチケット要求を受けた後，上記のような仕組みによって，配布するチケットを決定する．

以上のようなサブジェクト定義/コンディション定義の柔軟性によって，RightsShellでは，以下に例示するように，多様なビジネスルールに対応できる．

- 会員制モデル：会員のユーザIDをDB化しておき，その内容をサブジェクトとして定義する．
- 販売モデル：コンディション(課金方法)に「売り切り」を指定する．
- レンタルモデル：コンディション(利用期間)に，貸し出し期間を指定する．
- PayTVモデル：コンディション(利用回数)に「1回」を指定する．

4 頒布権管理に向けた拡張

この節では，前節で述べたストリーミングRightsShellを拡張し，ISPが個別に管理していたコンテンツのビジネスルールを，CPが管理するシステムについて説明する．

本システムは，前節で述べた基本構成に加えて，SRSソースサーバを設ける(図2)．SRSソースサーバとチケットサーバはCPが運用し，SRSサーバはISPが運用する．

今，CPとISPとの間で，あるコンテンツ(コンテンツIDをCとする)の配信契約が成立したものとする．CPがISPへコンテンツCを配送する際，SRSソースサーバは以下のような処理を行う．

1. 鍵$K_{C,ISP}$と，修正コンテンツID C_{ISP}とを生成する．
2. 配信期間などのビジネスルールを記述したACLを作成し，C_{ISP}にバインドして，チケットサーバへ登録する．
3. C_{ISP}とチケットサーバ名とをISPに通知する．
4. コンテンツを$K_{C,ISP}$で暗号化し，ISPに渡す．

ISPは，CPから受け取ったC_{ISP}とチケットサーバ名とに加えて，SRSサーバ名を含むメタファイルを作成する．また，CPから受けとった暗号化コンテンツ$E[K_{C,ISP}](C)$をSRSサーバにセットする．

このように拡張されたストリーミングRightsShellは，CPがチケットサーバを運用するので，たとえISP側の配信管理に問題がある場合でも，CP–ISP間の配信契約を保証できる．したがって，本システムはCPの頒布権を保護することができる．

その他，以下のような特徴も併せて持つ．

- CPは，ISP毎に異なるビジネスルールを設定できるため，利用期間をずらすなどの対応によって，同タイトルのコンテンツでも複数のISPに提供できる．
- ISP内のDBを参照できるよう構成することで，3節で述べたような，エンドユーザに対する細かな利用制御も可能となる．

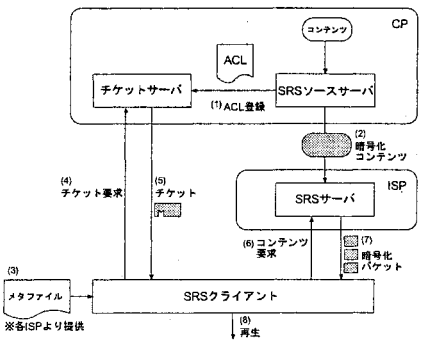

図2: 拡張されたストリーミングRightsShell

5 おわりに

本稿では，まず，ストリーミングサービス一般について，(1)多様なビジネスモデルに対応できる柔軟な利用/課金制御の課題，(2)CPによる頒布権管理の課題を示した．

次に，課題(1)に対する解として，チケットサーバによる柔軟な利用/課金制御が可能なストリーミングRightsShellについて説明した．また，課題(2)を解決するため，ISPによるコンテンツ配信をCPが集中管理するための拡張方式を提案した．

参考文献

[1] 中江他，カプセル化コンテンツ流通基盤(2)–チケットによる利用制御方式–，情処全大-57，1K-8，1998．
[2] 岡城他，動的な条件設定によるカプセル化コンテンツの利用制御，情処全大-60，5N-8，2000．