ブロードバンドにおけるマルチメディアストリーミング技術その3
～デジタルライツマネジメント（DRM）システム～

山本　秀樹

ブロードバンドの普及に伴って，ソフトウェアやゲーム，ビデオ等のデジタル・コンテンツを流通させるサービス（コンテンツ流通）が実際に始まってきた。しかし，デジタル化されたコンテンツは簡単にコピーができることから，コンテンツの権利保持者はコンテンツ流通に関しては積極的ではない。コンテンツ保護の観点からコンテンツ配信システムに必要な機能として，配信者に与えられている著作権情報の一元管理，著作権情報に基づいた配信サーバの制御，およびストリームの暗号化が必要である。本稿ではOKI MediaServer上に実装したこれらの機能について述べる。

著作権管理システム

ネットワーク上の不正コピーの防止にはまず個々の著作物の著作権がどのようになっているかを調べられるようにすることが重要である。著作権管理システムは，デジタルコンテンツの著作権情報を一元管理することを目的としている。著作権管理システムは，

①著作権情報を管理するDB

② DBの情報とコンテンツを結びつける手段

③コンテンツに一意に識別可能なIDを付与する機能

が必要になる。以下では我々が開発した著作権管理システムについて述べる。

（1）著作権管理システムの概要

上記の要求を満たすシステムとして，コンテンツIDフォーラム（cIDf）仕様[1]に基づくシステムを開発した。cIDfはデジタルコンテンツの流通促進を目的として設立された団体であり，著作権情報のフォーマット，著作権情報を識別するID番号のフォーマット，それらの管理方法などを定めている。

著作権情報は表1に示す構成になっている。著作権情報中のIDセンタ管理番号は世界で一意の番号となるために表2に示す構成になっている。地域コードは国などの単位で付与される。

cIDfの仕様では，IDセンタ管理番号は，コンテンツの流通条件が変わるたびに別のIDを払い出すことになっている。また，コンテンツとIDセンタ管理番号の関係付けを行うために，オプションとしてIDセンタ管理番号を電子透かしとしてコンテンツに埋め込む。

表1　cIDfの著作権情報の構成

項目名	意味・説明
IDセンタ管理番号	コンテンツを特定する全世界でユニークな番号であり、コンテンツID申請時に設定される。
コンテンツ属性	コンテンツ内容・種別を表す情報
権利属性	コンテンツに関わる権利の情報
権利運用属性	権利の許諾・委任・譲渡に関する情報
流通・分配属性	コンテンツ流通時に参照される情報

表2　IDセンタ管理番号の構成

項目名	意味・説明	サイズ（bit）
バージョン番号	IDセンタ管理番号のバージョンを既定	4
地域コード	IDセンタが存在する場所を識別する番号	4
センター番号	IDセンタの番号	8
センタ内番号	IDセンタが管理するコンテンツを識別する番号	任意

（2）VODシステムと著作権管理システムの統合

VODシステムで配信されるコンテンツに対して，著作権情報の登録と電子透かし埋め込みを行うシステムを開発した。システムの構成を図1に示す[2]。

コンテンツの流通条件が新たに追加されるごとに電子透かしを埋め込む必要があるが，このシステムでは著作権管理システムとVODを密に結合することで著作権管理システムはVODからコンテンツを入手し，著作権情報付与後，すなわち電子透かしを埋め込んだ後，そのデータを自動的にVODサーバに戻すようになっている。

データの流れを簡単に示す。①ではコンテンツは電子透かしの無い状態でVODシステムへ投入される。そのコンテンツの著作権情報をDBに登録しID番号を発行する

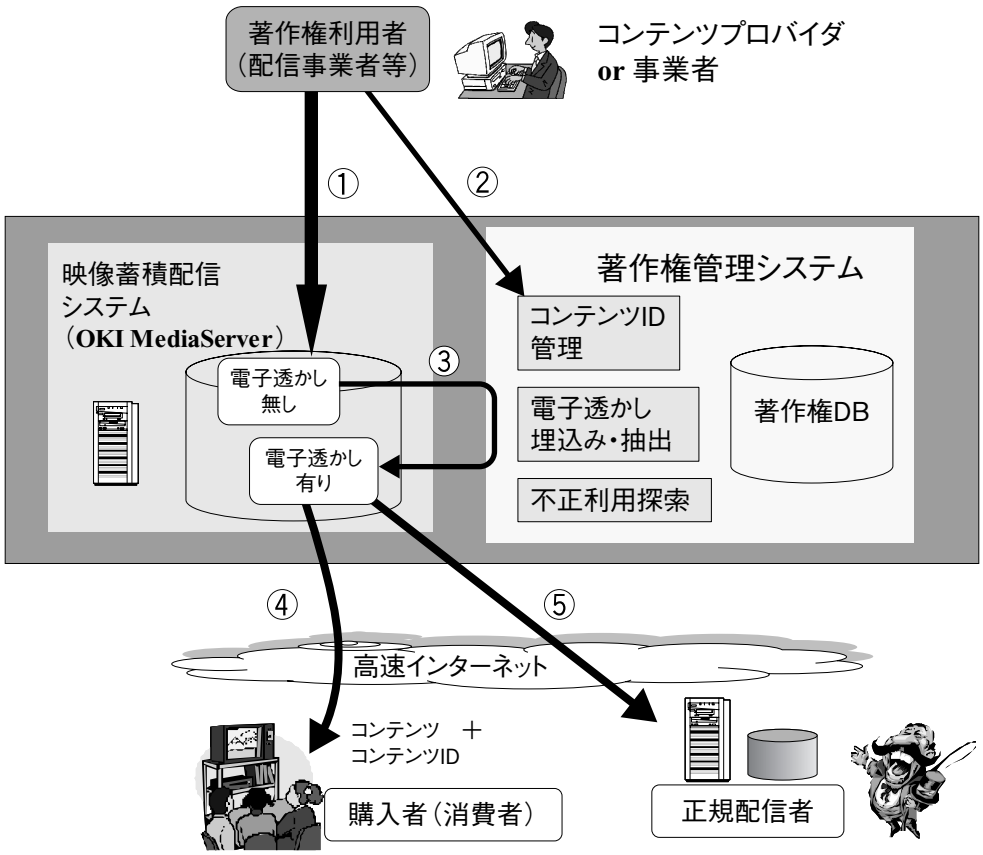

図1　著作権管理システムと映像配信システム[2)]

②。③では電子透かしをコンテンツに埋め込む。配信は電子透かしを埋め込まれたコンテンツのみ行う④。配信システムを分散する場合には電子透かしを埋め込まれたコンテンツを分散先に配布する⑤。この方式によって，著作権利用者は，同一コンテンツに対して流通条件やビットレートが異なる場合でも，一度VODサーバに投入したコンテンツに対し新たにIDを発行する操作だけを行えばよい。

(3) 適用例

本システムは，コンテンツ流通実証実験推進協議会のビデオストリーミング実験[3)] において，1年間ニュース映像コンテンツに対する著作権情報の発行と電子透かしの埋め込みに使用された。また，インターネットでの映画試写会でも使用された。これらを通じて実用的に使用可能なことが検証された。

さらに，ID管理センターが複数ネットワーク上に存在する場合にどのセンターから著作権情報を引き出せばよいかを決定するシステム（Resolution System 略してRA）との結合についても財団法人デジタルコンテンツ協会等との実証実験にて検証している[4)]（図2)。

ライセンス管理

映像配信システムを使ったコンテンツの有償配信サ-ビスには，販売用の視聴ライセンスの定義機能，販売したライセンスに基づいた配信サーバの制御機能や課金・認証機能が必要になる。以下ではこれらの機能について述べる。

(1) 視聴ライセンスの付与単位

コンテンツ流通では，レンタルビデオのように物流を伴わないため，複数コンテンツを簡単にまとめて販売したり購入したりできる。そこで，本システムでは視聴ライセンスを付与する対象を，図3に示すように個々のコンテンツではなくコンテンツグループとすることにした。例えば，刑事物パックや，西部劇パックといったグループを作ってそれに対して価格を設定することができる。コンテンツグループが1つのコンテンツしか含まないときは一つのコンテンツに対してライセンスを定義していることになる。コンテンツグループに対する操作として次の機能を用意している。

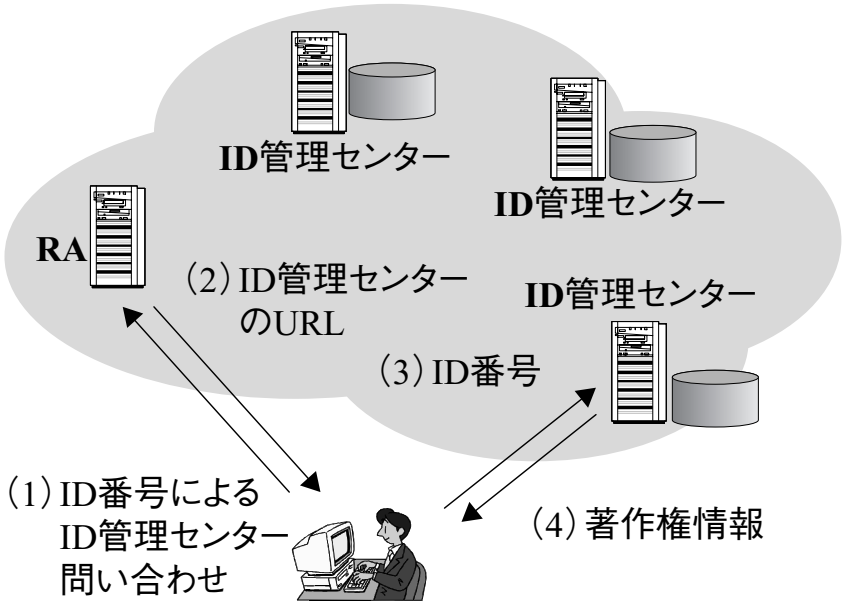

図2　RA実験システムの構成

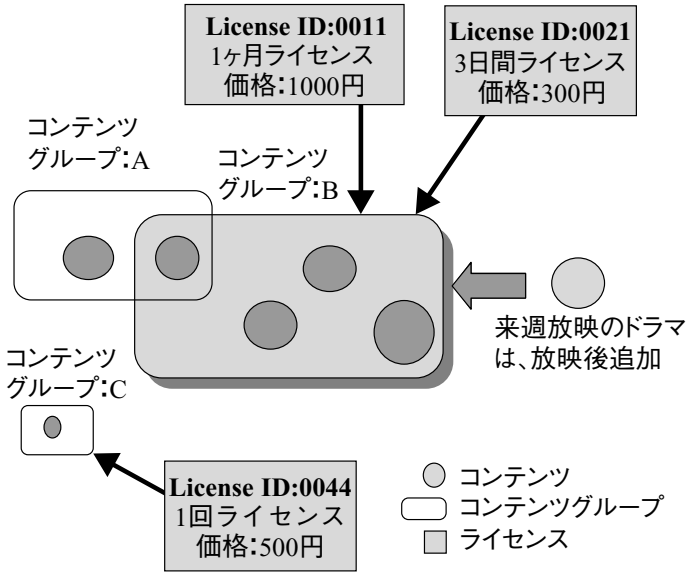

図3　コンテンツグループとライセンスの関係

①グループへのコンテンツ追加機能

連続番組やサッカーのJリーグ・パックなどのように後からコンテンツが追加されるものがある。グループへのコンテンツの追加はサービス上利用者の不利益にならないのでシステムとしては制限しない。

②グループメンバーの変更の制御

ライセンス販売後，コンテンツグループからメンバーを削除したり変更するのは既存の購入者（視聴者）にとっ

て不利益になるため，オペレータがそのような処理をすることはできないようにしている。ただし，販売開始前のコンテンツグループに対してはメンバーの削除を許可している。

(2) ライセンスの種類

ライセンスの種類を表3に示す。

視聴ライセンスは，(1) で述べたコンテンツグループに対して定義することができる。1つのコンテンツグループに対して複数のライセンスを定義することができる。ライセンス情報およびライセンスの購入履歴（契約情報と呼ぶ）はデータベース上に管理される。契約情報の概略構成を表4に示す。

表3　視聴ライセンスの種類

項目名	意味・説明
回数制限	視聴回数を制限するライセンス。再生を開始した時点で1回とみなされる。
期間制限	ライセンスを購入してから決められた期間だけ視聴できるライセンス。
定期購読	期間制限のライセンスで、期間がすぎると自動的に契約が更新されるタイプのライセンス。明示的に契約解除をするまで自動的に継続される。

表4　契約情報の概略構成

項目名	意味・説明
契約ID	視聴契約を一意に識別するID
ライセンスID	ライセンスの種別を示すID。このIDでDBを検索すると詳細な情報が得られる。
ユーザID	ライセンスを購入したユーザのID
契約日時	ライセンスを購入した日時
初回視聴日	購入後、初めて視聴した日時
販売金額	ライセンスの価格

(3) ライセンスに基づいた配信サーバの制御

配信サーバは，ライセンス管理対象のコンテンツに対する配信要求に対して，配信開始時にはそのユーザが有効なライセンスを持っているかどうかをチェックし，配信を開始する。さらに配信中にライセンス期間が切れた場合には配信を停止する。

実際のサービスでは，サービス事業者のサポート窓口に「誤って購入してしまったのでキャンセルしたい」といった要求が来ることがある。ISP側としてはそのユーザが一度も視聴していなければキャンセルを受け付けることがある。このような場合を想定して契約情報には初回視聴日時フィールドを用意している。

(4) 課金・認証インタフェース機能

ユーザごとの課金情報は，リレーショナル・データベース（RDB）上に格納されている契約情報を集計することによって得られる。そのため，サービス事業者側の課金システムとのインタフェースは容易に作成可能である。

視聴ユーザがライセンスを購入する場合，および購入したライセンスを使って視聴する場合にはユーザ認証が必要になる。OKI MediaServerは小規模サービス向けに内部に認証DBを持つ。ISPなどでの使用時には，外部認証サーバをアクセスするように設定することができる。認証サーバとのインタフェースとしては，RADIUS，LDAP用のサンプルが用意されている。

(5) ライセンス管理の適用例

ライセンス管理機能を組み込んだ分散配信サーバOKI MediaServerの概略構成と，視聴者がライセンスを購入して視聴するまでのデータの流れを図4に示す。図中の緑の部分がOKI MediaServerのモジュールである。コンテンツポータルはWebサーバ上のコンテンツ一覧であり通常サービス事業者側が構築する。認証サーバも同様にサービス事業者側にあらかじめ存在していることが多いため，この図ではOKI MediaServerの認証モジュールからアクセスするようになっている。認証モジュールはCGIとして提供されているため，コンテンツポータル側で実行することも可能である。以下に視聴までの流れを示す。

①視聴ユーザは，コンテンツポータル上に提示されているライセンス情報，すわなちコンテンツグループ，値段，期限などの情報から，購入するものを選択する（視聴契約）。サーバ側では，そのユーザの認証を行い，認証されれば，指定されたライセンスに対する契約情報を作成しDBに追加する。データベースに契約情報が追加された時点でシステム上は契約が成立したことになる。

②契約後ユーザが実際に視聴したいコンテンツを選択すると，購入から時間が経過していた場合はサーバ側では再度認証を実行してから視聴処理を行う。視聴処理ではDBを検索することで，そのユーザがすでに指定されたライセンスを購入し，かつそのライセンスが有効期間内であるかをチェックする。有効期間内であれば配信に必要な情報をプレーヤ側に送ると同時に，配信サーバに対して配信指示を出す。分散構成の場合は，配信指示は，視聴ユーザの最寄のローカルサーバに出される。

③ローカルサーバは配信指示に従って視聴ユーザの端末に対して配信を開始する。配信指示には，ライセンス情報から算出される配信期限の情報が含まれている。例えば，2002年9月10日18:00に購入した3日間有効のラ

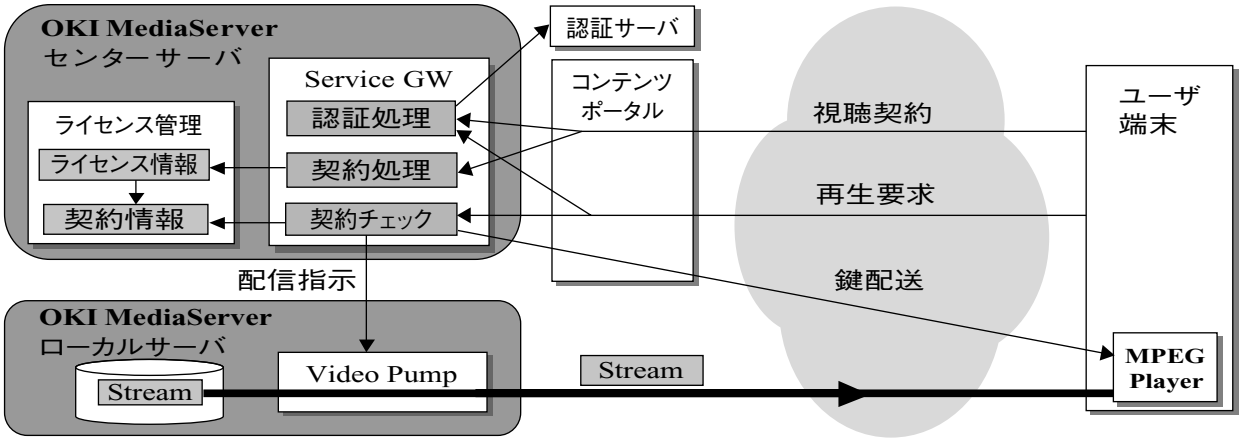

図4　OKI MediaServerにおけるライセンス管理の使用例

イセンスの場合，配信期限は2002年9月13日18:00である。この時間になると，ローカルサーバの配信モジュール（Video Pump）は配信を中断する。

ほぼこの図と同様の構成のシステムは，実際の大手サービスプロバイダーの有償コンテンツ配信サービスに採用されている。

通信路の暗号化

OKI MediaSeverによるストリーミング配信では，ユーザ端末上にコンテンツが蓄積されることはなく，受信したデータはすぐに再生され保持されない。そのため，ダウンロード型の配信サーバと比較するとコンテンツの保護の面で優れているといえるが，盗聴などの不正アクセスからコンテンツを守るために通信路の暗号化機能を提供している。

図4の例では，次の個所で暗号化通信を行う。

①視聴契約時，再視聴時のユーザ端末からコンテンツポータルへの認証情報の通信。

②Service GatewayからMPEG Playerへの鍵情報の通信。ここで鍵情報は，暗号化されたストリームをデコー

TIPS【動向と用語解説】

動向

DRMとしてMicrosoftのWindows Media Technologyがあるが，これはライセンス管理のためのライブラリ群であり実際の商用サービスを構築するためにはソフトウェア開発がかなり必要である。OKI MediaServerのライセンス管理システムおよびストリームの暗号化技術は，サービスをすぐに実現することが可能なレベルのパッケージとして構築されている。ライセンスの種類としてほぼ実際のコンテンツ関連のサービス（雑誌，レンタルビデオなど）の販売形態を網羅している点に特長がある。また，認証，課金インタフェースは標準のプロトコルをサポートしており簡単に既存のシステムに結合可能である。

著作権管理システムのための記述形式に関しては，現在cIDf，MPEG-21，TV-Anytime Forumなどで標準化が進められている。本稿ではcIDf仕様を実装した例を示したが，OKI MediaServer自体はXMLで記述されたメタデータを簡単に扱えるようになっているため標準化の普及動向にあわせて柔軟に対応することができる。

用語

RADIUS：Remote Authentication Dial In User Serviceの略。ダイアルアップサービスなどのユーザ認証のプロトコルとして既定されている。IETFの標準。RFC2058，2865，2866，2869など。

LDAP：Lightweight Directory Access Protocolの略。インターネットのディレクトリサービスのためのプロトコル。現在V3が主流。

ドするために必要な鍵である。

③Video PumpからMPEG Playerに送信するストリーム情報。共通鍵暗号をベースの暗号化を行っている[5]。ストリーム情報の暗号化は，蓄積コンテンツだけでなく，リアルタイム映像コンテンツに対しても行うことができる。

また，図1の著作権管理システムでは著作権情報の登録時には暗号化通信を用いる。

お わ り に

本稿では，コンテンツ流通の実現に必要なデジタルライツマネージメント（DRM）技術として，著作権管理システム，ライセンス管理システムおよび通信路の暗号化について述べた。これらの技術によりOKI MediaServerを用いて，安全なコンテンツ配信サービスを行うことができる。なお，本稿では言及しなかったが，コンテンツ保護としては，コンテンツの原本（テープなど）の管理やサーバ管理者の管理など運用面での対策も重要である。

現在，DRM関係のメタデータの標準化が，TV-Anytime Forum[6]，MPEG-21[7]，cIDfなどで積極的に進められている。本稿ではcIDfの実装例を示したが，OKI MediaServer自体のメタデータ管理機能は各種XMLドキュメントを格納可能であるため他の標準のメタデータも容易に扱うことができると考えられる。今後はこれらの標準化に積極的に関与するとともに最新技術を実装した製品を提供していく予定である。 ◆◆

■参考文献

1）コンテンツIDフォーラム：http://www.cidf.org/
2）近藤，佐藤，山本，長坂：著作権管理システムを統合した映像配信システム，電子情報通信学会2001年ソサエティ大会B-16-2，2001年
3）ビデオストリーミング実験グループ：ブロードバンド・インターネットを利用した分散型映像コンテンツ配信の公開実験を開始，
http://www.vsforum.org/home/whats/release-exp-20010423.html，2001年
4）山本，内田他：コンテンツ流通促進のための基盤システム，IPA平成13年度成果報告集，2002年
5）佐藤，山本，長坂：MPEGストリーミングのためのブロック暗号処理方式，情報処理学会第1回FIT大会予稿集，2002年
6）TV-Anytime Forum :http://www.tv-anytime.org/，2002年
7）MPEG: “MPEG-21 Overview”，http://mpeg.cselt.it/，2001年

●筆者紹介

山本秀樹：Hideki Yamamoto.ブロードバンドメディアカンパニー メディアソリューション部