1K－8

# 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－

中江政行 細見格 市山俊治
NEC ヒューマンメディア研究所

## 1 はじめに

別稿[1]で述べたカプセル化コンテンツ流通基盤における利用/課金制御方式について述べる．本方式では，コンテンツの利用許可証(チケット)の販売により利用/課金制御を行う．

本方式の特徴は，コンテンツの構成要素ごとに利用条件と課金条件を設定できる点にあり，従来方式に比べ，より柔軟な利用/課金制御を可能にする．構成要素ごとの利用条件および課金条件は，アクセスコントロールリスト（ACL）を用いて記述される．ACLをカプセルから分離し信頼できるチケットサーバで管理することで，カプセル化コンテンツの高い安全性を実現できる．

本稿では，コンテンツのカプセル化形式と，チケット方式によるコンテンツ利用制御機構について述べる．

## 2 コンテンツ流通システム

本システムは，コンテンツ視聴に用いる「ビューワ」，エディタ等で作成されたコンテンツのカプセル化を行う「カプセルジェネレータ」，ACL管理とチケット配信を行う「チケットサーバ」，利用料金の振込処理を行う「決済サーバ」，カプセル化されたコンテンツデータとその操作メソッドから成る「MediaShellコンテナ」から構成される(図1)．

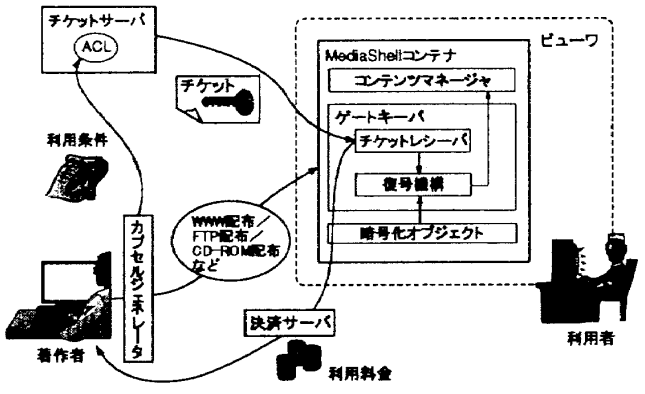


図 1: システム構成

## 3 MediaShellコンテナ

MediaShellは我々が提案するマルチメディアコンテンツカプセル化技術であり，コンテンツの構成要素ごとの利用/課金制御などを特徴とする[1][2].

利用／課金制御の対象を「(要素)オブジェクト」と呼ぶ．オブジェクトとして何を選ぶかは，コンテンツの性格によるが，例えばWWWコンテンツの場合，1つのhtmlファイルもしくは1つの埋め込みデータ（画像ファイル／動画ファイル等）とすることができる．

MediaShellコンテナは，以下のような構造をもつ．

- MediaShellコンテナは，各オブジェクトに対応した複数のゲートキーパと，それらを束ねる1つのコンテンツマネージャとをもつ．
- コンテンツマネージャはゲートキーパへのオブジェクトデータ要求を行い，表示イメージの生成を行う．
- ゲートキーパは1つの暗号化オブジェクトデータと関連づけられており，チケット要求/受信を行うチケットレシーバとオブジェクトデータ復号を行う復号機構により，コンテンツマネージャへのオブジェクトデータ出力を制御する．

各ゲートキーパがもつ復号機構では，関連づけられた暗号化オブジェクトに関する以下のような情報が保持されている．

- 著作権情報（著作者名，作成日時，オブジェクト名など）
- 利用鍵テーブル（利用法／利用鍵）

利用鍵は，それぞれ一つの利用法に対応づけされている．利用法$U$に対応する利用鍵$K_U$は，一方向性ハッシュ関数$hash$を用いて$K_U = hash(著作権情報|U)$と表される．

暗号化オブジェクトデータは，慣用暗号により暗号化されたオブジェクトデータである．その際に用いられる鍵は乱数により決定される．この鍵をオブジェクト鍵($K_{obj}$)と呼ぶ．

## 4 利用制御方式

### 4.1 チケット方式

MediaShellコンテナは，任意のftpサイトやWWWサイトを通じて，自由に配送される．そして，利用者がコンテナ内のコンテンツを利用する際に，その旨をチケットサーバに要求し，特定のチケットを取得してはじめて利用できる仕組みになっている．一方，チケットサーバは，利用者からの要求と要求対象であるコンテンツの利用条件とを照合し，条件に合致する要求に対してのみ適切なチケットを生成／配信する．

A Capsulated Content Distribution Architecture (2)
–On-demand Access Control with Tickets–,
Masayuki Nakae, Itaru Hosomi, Shunji Ichiyama,
Human Media Research Laboratories, NEC Corporation.

チケットによる利用制御方式は，以下のような特徴をもつ．

- 従来コンテナ内に同梱されていた利用条件を，信頼できるチケットサーバに管理させることで，より高い安全性を実現できる．
- 利用条件をオブジェクトおよび利用方法ごとに記述できるようにすることで，利用制御の柔軟性を向上させることができる．例えば，オブジェクトごとにペイパービュー／時間課金など，異なる課金方法を選択できる．
- チケット鍵分割により，二次著作物の著作権保護および流通を可能とする．

以下の項では，柔軟な利用条件記述を可能にするACLについて説明し，チケット送受とコンテンツ利用について説明する．

### 4.2 ACL

ACLでは，オブジェクトごとに利用条件とチケット鍵との組を記述していく．利用条件は，例えば，

```
picture.gif {                          #対象オブジェクト名
  View {                               #閲覧に関する条件記述
    cond {                             #利用条件
      Resolution <= 640x480            #解像度の上限
      ColorDepth <= 16                 #色数の上限
      Price = 3                        #課金額
      PaymentWay = PayPerView          #課金方法
    }
    key {                              #チケット鍵定義
      9AFB38A2
    }
  }
  Print {                              #印刷に関する条件記述
  ...
  }
}
```

といったように記述される．この例において，オブジェクトpicture.gifの閲覧に関する利用条件は，「表示解像度の上限を640x480とし，表示色数の上限を16とする．課金額は3円で，課金方法はペイパービューである．」と解釈される．

オブジェクト$obj$/利用法$U$に対応するチケット鍵$K_{T(obj,U)}$は，$K_{T(obj,U)} = \{K_{obj}\}_{K_U}$で表される．ここで，$\{D\}_K$はデータ$D$を鍵$K$で慣用暗号により暗号化することを示す．

### 4.3 チケット送受およびコンテンツ利用

チケット送受およびコンテンツの利用における大まかな処理の流れを図2に示す．利用者がMediaShell形式のコンテンツのあるオブジェクトを利用する際，対応するゲートキーパは解像度や色数などの端末情報を含んだ利用要求を生成し，チケットサーバに渡す．

要求を受け取ったチケットサーバはACLと要求とを照合して，条件が満された場合にのみ，以下のような構造をもつチケットを生成し，配信する．

- チケット発行者名
- 発行年月日
- 利用を許可するオブジェクト名$obj$
- 許可する利用法$U$
- 利用料金(=課金額)
- 料金支払方法(=課金方法)
- チケット鍵$K_{T(obj,U)}$
- 発行者によるデジタル署名

ゲートキーパは，チケットレシーバによりチケットを受け取り，署名による正当性の検証を行った上で，チケットに含まれるチケット鍵を取り出し，復号機構へ渡す．復号機構ではチケット鍵$K_{T(obj,U)}$・利用鍵$K_U$・暗号化オブジェクトデータ$obj'$から，次式で表される操作を行って，オブジェクトデータ$obj$を復元する．

$$K_{obj} = \{K_{T(obj,U)}\}_{K_U}$$
$$obj = \{obj'\}_{K_{obj}}$$

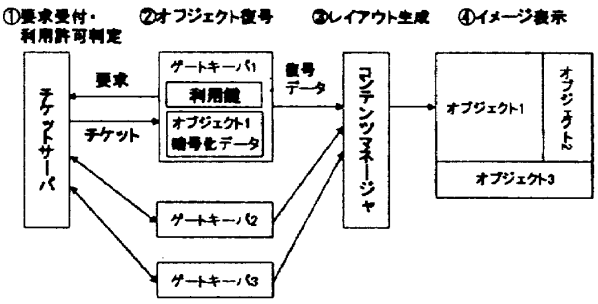


図 2: チケット送受およびコンテンツ利用

## 5 おわりに

本流通システムでは，次のような工夫により，安全性の高い利用制御を実現した：(1) 要素オブジェクトごとに異なるオブジェクト鍵で暗号化，(2) オブジェクト鍵の取引ではなく利用法に依存したチケット鍵を取引，(3) 適切なチケット鍵と利用鍵の組合せでのみオブジェクト鍵を復元可能．

また，次のような工夫により，利用条件の柔軟性と安全性を高めた：(1) 利用/課金条件をコンテンツ単位でなく，オブジェクトと利用法の単位で記述，(2)ACLをコンテンツから分離し，信頼できるチケットサーバに管理を委託．

## 参考文献

[1] 細見, 中江, 市山, 「カプセル化コンテンツ流通基盤(1) −全体構成と利用状況適応機能−」, 第57回情処全国大会, 1998.

[2] 細見, 谷, 市山, 「多様な再生環境に適応する流通コンテンツ・アーキテクチャの提案」, 第55回情処全国大会, 1997.