

デジタル情報流通アーキテクチャ MediaShell と その利用・課金制御

細見 格、中江 政行、市山 俊治
NECヒューマンメディア研究所

我々はカプセル化されたデジタル情報のコンテナおよび流通アーキテクチャを開発しており、その主な特徴は流通するコンテンツに対してその構成要素毎に利用方法や課金方法を指定でき、且つ消費者がそれらを簡単に選択できる点にある。本稿では、主にチケットを用いた間接的なコンテンツ販売による柔軟な利用制御と課金制御、および端末システムのスペックに応じて各コンテナ自身で表示内容を最適化する適応表示制御について述べる。

Digital Information Logistics Architecture "MediaShell" And Its Billing and Utilizing Management

Itaru Hosomi, Masayuki Nakae, Shunji Ichiyama
Human Media Res. Labs., NEC Corp.

We are designing a capsulated digital information container and its logistics architecture. Main features of the container and the architecture are having variety of means of utilizing and billing for each element of digital contents, which can be selected easily by consumers. In this paper, we describe capabilities of the architecture - especially flexible control to use and pay for digital contents, and the container's adaptive control to display contents on various terminal systems.

1 はじめに

インターネット上でのデジタル商品の販売は、物流によるパッケージ商品の販売に比べ、量産や運送、在庫管理などのコストが大幅に削減できる流通手段として期待されている。しかしながら、インターネット上で流通する商品や電子マネーの安全性、端末システムの種類の多さや操作の難しさ、誤操作による危険性など問題点も多い。

我々は、デジタルコンテンツを流通させる上で、コンテンツの提供者に対してはその権利と利益を保護し、利用者に対してはできる限り簡単且つ効果的に各コンテンツによるサービスを提供するための技術開発を行っている。本稿では、特にデジタルコンテンツの利用制御と各利用形態に応じた課金制御について議論する。

2 カプセル化コンテンツの流通

デジタルコンテンツは、一旦入手すればその正確な複製や改竄が容易である。このためコンテンツを暗号化し、その制御情報や管理情報とともにパッケージ化して流通させるカプセル化技術が数多く提案／利用されている[1][2]。

カプセル化されたコンテンツ(以下カプセル化コンテンツ)は、それ自体の複製は容

易だが暗号化されているため正規の手続きにより復号しなければ利用できない。したがって、代金と交換で復号鍵を発行することにより、コンテンツ自体が複製されてもそれらが利用された数だけ料金の徴収が可能である。しかし逆に、カプセル化されることでデジタルであることの柔軟性を損なう面も多い。

3 デジタル情報流通アーキテクチャ

そこで我々は、デジタルコンテンツの利用における安全性と柔軟性を両立可能なデジタル情報流通アーキテクチャ MediaShell を提案し、そのシステム試作を行なっている。図1に示すように、MediaShell ではコンテンツ自体とは別経路でチケットと呼ぶコンテンツの「利用券」を販売する。各チケットにはコンテンツの復号鍵の他に利用条件や課金条件が記述されており、これらを各カプセル化コンテンツ自身が解釈してサービスを提供する点に特徴がある。

本アーキテクチャにおいて、利用者はまずコンテンツをオンラインもしくはオフラインで入手し、別途チケットをオンラインで購入することによりコンテンツを利用する。コンテンツの入手はそのメーカーや販売代理店の他、先にコンテンツを入手した一般利用者

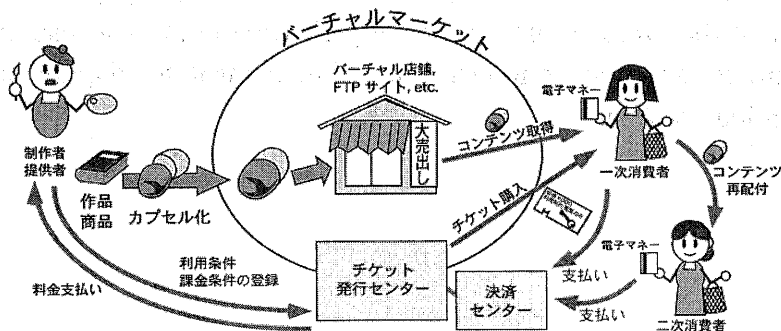


図1 デジタル情報流通アーキテクチャ MediaShell の概要構成

から複製物を貰ってもよい。一方、チケットについては必ずオンラインでチケット発行センター(チケットサーバ)に接続しなければならない。実際には、入手したカプセル化コンテンツに対して利用要求のメッセージを送るかコンテンツの視聴/実行を開始すると、自動的にカプセル化コンテンツがチケットサーバに接続して必要なチケットを入手し、チケットの記述に基づいて利用制御や課金を行なう。我々はこのような仕組みを含むカプセル化コンテンツのコンテナを設計、実装した。ただし、本稿において「コンテナ」とはコンテンツをカプセル化する際の入れ物であり、コンテンツを管理・操作する各種の機能を含むものとする。

3.1 カプセル化コンテンツの構造

MediaShellアーキテクチャでは、その主要な機能の大半をカプセル化コンテンツのコンテナに持たせている。MediaShellではコンテンツを図2のような構造でカプセル化し、流通させる[3]。

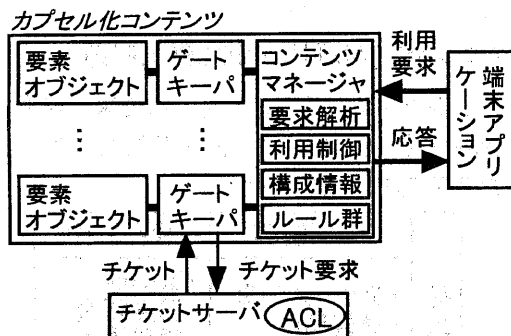


図2 MediaShellのカプセルの構造

図2で「要素オブジェクト」とは、1つのコンテンツを構成する1つ以上の要素を表し、それぞれ個別に暗号化されている。各要素オブジェクトはコンテンツをカプセル化する際に適当な単位で設定する。「ゲートキーパ」は、各要素オブジェクトへのアクセス認証や要素オブジェクトの復号、コンテンツ外部か

らの要求内容に応じた変更操作などを行なう機能モジュールである。「コンテンツマネージャ」は1つのコンテンツ全体を管理し、コンテンツへの外部からのアクセス要求の解釈、各ゲートキーパへの指示、コンテンツの出力時の構成制御、プロファイル情報の管理・提供などを行なう。

3.2 要求メッセージ

カプセル化コンテンツへの要求メッセージは以下のようなスクリプトで表現する。

```
例: play adaptive
    format HTML
    condition client.disp.width="640"
    and client.disp.height="480"
    and client.soundout="yes";
```

最初の play コマンドには normal と adaptive のいずれかの引数を与える。normal ではコンテンツの初期設定に従って内容を出力し、adaptive では condition 以下の端末システム条件に適合するようにコンテンツマネージャが出力内容を調整する。format コマンドは出力フォーマットを指定するものだが、現在は HTML のみに対応している。

3.3 チケット方式と ACL

前述のチケットはコンテンツの各要素オブジェクト毎に発行され、1つの要素オブジェクトに対してその利用条件毎に複数種類のチケットを用意しておくことができる。利用条件は例えば次のような観点から設定することができる。

- ・利用者(年齢/所属等)
- ・コース(松/竹/梅コース等)
- ・用途(画面閲覧のみ/印刷可能等)

利用条件や課金条件は、チケットサーバ上に ACL(アクセス制御リスト)と呼ぶ形式で該当する要素オブジェクトの復号鍵とともに記録している。ACL はコンテンツの提供者が作成してチケットサーバに登録する。

利用者が、入手したカプセル化コンテンツに対して利用要求メッセージを送ったり実行や再生を要求すると、カプセル化コンテンツ内のコンテンツマネージャがそれらの要求内容を解釈し、適当なゲートキーパに対して必要な要素オブジェクトの提出を指示する。指示を受けたゲートキーパはチケットサーバに接続して利用者のIDと要求内容を送り、チケットサーバは要求内容に対応する利用条件を持った ACL を解釈して以下の手順でチケットを発行する(図2参照)。

1. 要求元のユーザ認証により、チケットを発行して良いか否かを判定
2. 発行を許可した場合、ACL から適当な復号鍵を抽出
3. 復号鍵をその発行記録(発行年月日など)とともに利用者の公開鍵により暗号化したチケットとして発行

ゲートキーパは発行されたチケットを受け取って要素オブジェクトを復号し、コンテンツマネージャに渡す。

3.4 端末上での出力制御

以上のようにして出力を許可された各要素オブジェクトを、コンテンツマネージャが統合して端末上に出力する。このとき、コンテンツマネージャは要素オブジェクトの構成を端末システムのスペックに応じて操作することができる。このような機能の1つとして、現状では各要素オブジェクトの表示構成を様々な端末システムの画面に適応させる適応表示制御を実現している。適応表示制御によって、画面解像度の低い端末でも操作性の低下を抑えたり、見てもらうべき広告が隠れてしまわないようにすることができる。

3.5 セキュリティへの対応

各要素オブジェクトは 56 ビット DES 慣用鍵で暗号化している。一方、要素オブジェク

トの復号鍵を含むチケットは 512 ビット RSA 公開鍵暗号を用いてチケット発行時に利用者の公開鍵で暗号化している。チケットはカプセル内のゲートキーパがチケットサーバに要求して入手し、ゲートキーパ内で使用される。利用者が自分でチケットを入手してコンテンツを復号する場合に比べて不正使用がより困難になっている。また、コンテンツは要素オブジェクト単位および利用法毎に異なる復号鍵で逐次復号されるため、1コンテンツを1つの鍵で復号する方式に比べて鍵の不正入手に対するリスクも比較的小さい。

現在、カプセルからの応答結果は HTTP プロトコルで Web ブラウザに出力している。従って、Web ブラウザの保存/複製機能を用いれば出力された内容を転用できる。専用のブラウザを用意したり、ブラウザの機能を制限するプログラムを併用することも考えられるが、まだそれらには着手していない。画面キャプチャによる複製までを考慮すると、各データ毎の電子透かし挿入や、端末の OS レベルでの制御が必要になる。

4 コンテンツの利用制御と課金制御

デジタルコンテンツに対する従来の利用制御や課金制御[4]と、我々が新たに対応した制御機能を図3に示す。

	利用制御	課金制御
従来	・アクセス制御 ・複製制限	・買い取り ・回数課金 ・期間課金
新規	・出力品質制御 ・適応表示制御	・混合課金 (要素単位)

図3 利用制御と課金制御の種類

MediaShell の利用制御および課金制御はいずれも要素オブジェクト単位で行なう。図3で出力品質制御とは、利用者の権限や発行されたチケットの種類により、出力する

要素オブジェクトのサイズを変更したり、代替オブジェクトを出力する機能である。すなわち、利用者の支払額(選択されたチケットの価格)やアクセス権限に応じた品質で出力することができる。一方、**適応表示制御**とは、端末システムのスペックに応じて表示内容を制御する機能である。端末システムのスペックは、端末システム側からメッセージとして受け取る。

また、課金制御の**混合課金**とは、要素オブジェクト毎に買い取り型や期間課金など1つのコンテンツ中で異なる課金手段を適用するものである。このような課金は要素オブジェクト毎に個別のチケットを発行するため可能となっているが、各チケットの発行は対応する要素オブジェクトの出力時にそれぞれゲートキーパが指示するため、利用者自身が個別に操作する必要はない。ただし、出力される要素オブジェクト毎の課金条件を利用者に適切に通知するように、予めコンテンツを設計しておく必要がある。

このような利用制御と課金制御の例として、Pay Per View (回数課金)のコンテンツ

を試作した。試作コンテンツでは、その視聴に対して発行するチケットに「松」「竹」「梅」の3ランクを設け、それぞれのランクに応じた内容と課金額でコンテンツを視聴できる。

ACL は図4のように記述している。

```

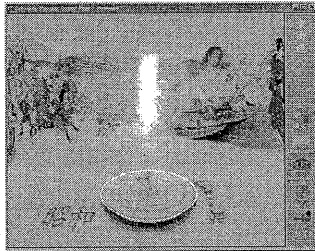
picture1.zip { # 要素オブジェクト名
  MatsuView { # 利用法(松コース閲覧)
    cond { # 利用条件定義
      Price = 200 # 課金額
      PaymentWay = PayPerView # 課金方法
    }
    key { # チケット鍵定義
      879074161041CBDD
    }
  }
  TakeView { # 利用法(竹コース閲覧)
    cond { # 利用条件定義
      Price = 50 # 課金額
      PaymentWay = PayPerView # 課金方法
      ...
    }
  }
  UmeView { # 利用法(梅コース閲覧)
    ...
  }
}

```

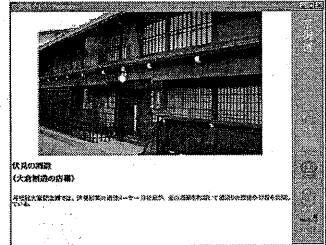
図4 試作コンテンツ用 ACL の一例

図5のコンテンツの例では、竹コースは再生中に広告が入ったり、写真の表示解像度や色数が変更されている。各写真が入ったページはそれぞれ個別の要素オブジェクト

松コース
(広告なし)



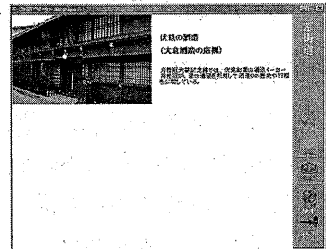
松コース
(高解像度)
(カラー)



竹コース
(広告あり)



竹コース
(低解像度)
(グレー)



写真提供: 外山達志

図5 松コースと竹コースによる表示内容の違い

として定義しており、1枚参照する毎にゲートキーパがチケットサーバにチケットを要求する。チケットサーバからは、指定されたコース(MatsuViewなど)のチケットがACLの内容に基づいて発行され、これを受け取ったゲートキーパが各コース別の料金を参照して課金が行われる。また、梅コースでは表示内容が簡略化される代わりに無料で視聴できる(図6)。

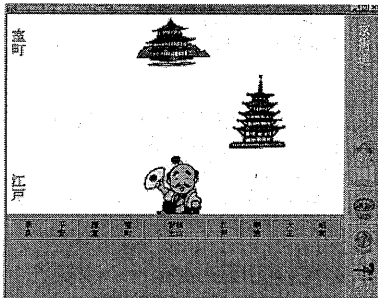


図6 梅コースにおける簡略化表示

これに対して以下の図7は、図6の内容を640x240の画面領域に表示した場合の適応表示制御の結果である。本文領域(背景が白い領域)の下部にあった時代選択のメニューが本文右側に縦型に表示されている。MediaShellでは、このような画面のレイアウト変更処理を次章で述べる方法によって実現している。

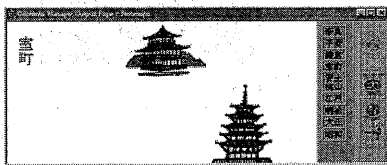


図7 適応表示制御の実行例

5 適応表示制御

コンテンツマネージャは、構成情報と呼ぶデータで要素オブジェクトの表示構成を管理しており、必要に応じて構成情報を変更することにより、上記の図7のように各端末画面の解像度や形状に適した構成で内容表示を行なうことができる。

5.1 オブジェクト構造の木構造化

カプセル内のコンテンツマネージャは、このような適応表示制御を実現するために要素オブジェクトの構成を木構造で管理し、ルールを用いて木構造を変更する。その後、変更した木構造を基に各要素オブジェクトを実際に構成して表示する。端末画面上での各要素オブジェクトの表示構成は、図8のような木構造で表現した構成情報として管理している。

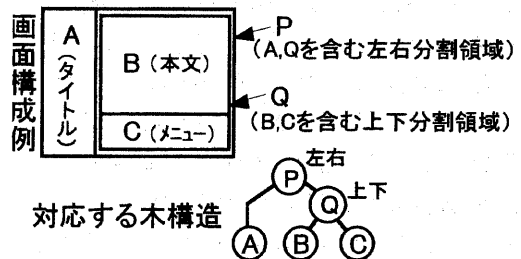


図8 画面表示時の要素構成と木構造

5.2 表示レイアウトの変更

適応表示のルールは、例えば次のように記述し、コンテンツマネージャが管理する。

```

1: cond="client.disp.height < profile.disp.height"
   // 条件: 端末画面の高さが必要解像度未満なら、
2: ope="horizontal gk03.menu"
   // メニューを90度配置変更
3: ope="reduce gk01.title" // タイトルを簡略表示

```

ルールは(*)の1:のような条件部と2:や3:のような適応化処理部からなる。適応化処理部は複数のメソッド(上記ルール中のhorizontalやreduceなど)を記述できる。

このようなルールに基づいて、コンテンツマネージャが要素オブジェクトの構成を表す木構造を変更する。

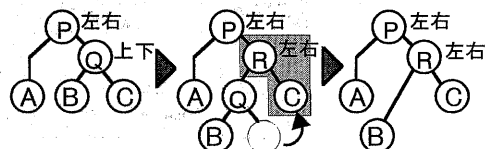


図9 ルール(*)と図8の例に基づく処理

図9はルール(*)の 2: で示した horizontal メソッドを実行した場合の処理である。このメソッドは、変更対象の表示要素と隣接する要素との位置関係を上下から左右に変更する。結果として、図10右側のように表示領域の高さの不足に対処したレイアウトとなる。

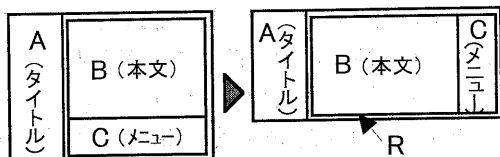


図 10 レイアウト変更結果

この他、現在の MediaShell の適応表示制御ではルール中で以下のようなメソッドを利用することができる。

popup	ポップアップ表示に変更
remove	指定オブジェクトを構成から削除
split	別ウインドウで独立表示
temporal	一定時間表示したのち消去
reduce	簡略型(小型)の代替要素を表示
fitdisp	画面サイズに合わせてリサイズ
vertical	左右配置から上下配置へ再編
horizontal	上下配置から左右配置へ再編

図 11 利用可能な適応処理メソッド一覧

5.3 コンテンツ制作者による制御

上記のルールでは、どのメソッドをどのような順序で記述するかによって適応表示制御の結果が異なるため、その結果がコンテンツ制作者の許容範囲で行なわれるよう配慮する必要がある。そこで、コンテンツ制作者が直接ルールを記述する他に、より簡便な手段としてルールはデフォルトの規則によって自動生成し、制約条件のみを制作者が記述することもできるようにした。

制約条件は、各要素オブジェクト間でどれがより重要(なるべく変更せずに表示したい)かを相対的な順序関係で表したものであり、例えば、

```
gk0001.priority > gk0002.priority
(gk0001, gk0002 は要素オブジェクト名)
```

のように記述する。ルールの適用時には、制約条件を参照して重要度の低い要素オブジェクトへの適応処理メソッドを先に実行する。

6 議論

MediaShell のアーキテクチャは、デジタルであることの自由度を活かすために柔軟な利用制御と端末システムへの適応機能を備える。本章ではそれらの特徴と流通市場について考慮すべき問題を議論する。

6.1 カプセル内処理による利用制御

本アーキテクチャでは、カプセル化コンテンツを先に入手し、そのカプセルに対して実行(再生)を要求すると必要なチケットをカプセル内のゲートキーパがチケットサーバから入手する。また、チケットに記述された利用条件に応じたコンテンツの出力形態のアレンジもカプセル内で行なう。利用者はあくまでカプセルと対話し、チケットの入手やコンテンツ出力時の変更手続きなどは利用者にも端末システムにも任せるとはしない。このようなアーキテクチャの利点および欠点には以下のようなものがある。

1. 要素オブジェクト毎に課金条件が異なる複雑な Pay Per Use にも対応可能
2. 特定のコンテンツに対して例外的な利用制御・課金制御を定義可能。
3. チケット入手や内容変更をカプセル外で行なわないため安全性が高い。
4. コンテナに多くの機能を持たせるため、カプセルが肥大しがち。
5. 複数のコンテンツを同時に利用する場合に機能リソースが冗長。
6. 複数の要素オブジェクトを連続的に出力する場合、何度も個別にチケットを要求するので実行効率が悪い。

端末適応機能は各端末システム上に実装した方が効率的ではあるが、本アーキテク

チャでは、コンテンツの利用に関してその制作者が(必要であれば)完全に制御できるようにするため、またコンテンツ単位で独自に機能を追加できるようにするために、可能な限りカプセル内で処理するようにしている。

上で列挙したように、MediaShellは運用上の効率が問題となるかもしれない。しかし今後のインフラ整備によって高速で安定したネットワーク環境が一般家庭レベルにまで広まれば、利用制御や課金制御の柔軟性に優れ、単一のコンテンツで多様な端末環境での利用に応じられるという点が多くコンテンツ制作者と利用者双方の利益になると期待している。また、そのためにはカプセルの構造や機能の複雑さや各種制御のための設定の煩わしさが負担とならぬようにツールやサービスを十分に提供し、それらの機能を積極的に活用してもらえよう配慮することが必須である。

6.2 適応表示制御と課金の問題

MediaShellの適応表示制御により、解像度や縦横比の異なる端末画面上でも可読性や操作性に配慮した内容表示が可能となる。しかし、各端末画面に適応するために表示する要素オブジェクトの配置を変更することは、各要素オブジェクトに設定された価格の妥当性に影響を及ぼすことも考えられる。

既存のメディアにおける記事や広告の掲載料については、例えば新聞やWWWのホームページでは紙面上の掲載位置やサイズ、色数などによって決まる。しかし、現状では異なるメディア、異なる表示形態に対して相互に課金額を換算する基準が無いため、各表示形態(画面上の一部に常時表示する場合や一定時間全画面表示して消去する場合など)についてそれぞれ広告主との契約が必要になる。これを、一定の基準と計算式によって課金額を導く方式で契約できるよ

う提案していく必要があるだろう。

7 おわりに

本稿では、カプセル化コンテンツをチケットの発行を通じて販売するデジタル情報流通アーキテクチャ MediaShell について述べ、特にそのコンテンツ利用制御と端末システムへの適応表示制御について詳説した。本アーキテクチャでは、デジタルコンテンツのカプセル化と暗号強度の高いチケットによる間接的な取引によって十分な安全性を確保しながら、チケットの内容を設定するACLと各カプセル内部の利用制御機能によって柔軟なコンテンツ利用と課金を可能にしている。さらに、端末システムのスペックに応じてコンテンツの表示構成を決定する適応表示制御によって、例えば十分な表示領域を持たない端末でも各表示要素の重要度や役割に応じた表示を可能にしている。

MediaShell が持つこのような柔軟性や適応能力を十分に発揮するために、ネットワークのインフラ整備と様々なメディアや表現間での一貫した課金・契約基準の整備が望まれる。

参考文献

- [1] Olin Sibert, et al. : Securing the Content, Not the Wire, for Information Commerce, <http://www.intertrust.com/star-lab.com/secure-the-content.html>
- [2] Shuichi Tashiro: Capability-Based Usage Control Scheme for Network-Transferred Objects, Inet97 proceedings, <http://www.isoc.org/inet97/proceedings/A4/A4.3.HTM>
- [3] 細見, 他: 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回情処全大講演論文集(分冊3), 6Q-5, pp.254-255, 1997.
- [4] 木島, 他: 超流通におけるコンテンツ流通のための課金機構の開発, <http://www.ipa.go.jp/NBP/CREC/Data/2-107/2-107.pdf>