ユーザ要求に適合したサービスを提供するカプセル化コンテンツ

中江 政行　　細見 格　　市山 俊治
日本電気株式会社 ヒューマンメディア研究所
{nakae, hosomi, ichiyama}@hml.cl.nec.co.jp

概要

本稿では，ユーザの利用時要求に合わせた様々なサービスの提供を可能とするための，カプセル化コンテンツの利用制御技術（チケット方式）について述べる．本方式では，一般的な超流通モデルと同様にコンテンツの構成要素データを暗号化しているが，その復号鍵から各種サービスに依存したデータ（チケット鍵）を生成し，各チケット鍵の配布条件や課金条件を個別に設定することで，各サービスの利用を限定的に許可し課金を行うことができる．このように安全で柔軟な利用制御により，カプセル化コンテンツの流通を促進することができる．

A Capsulated Content Providing Services Adaptable for Users' Requests

Masayuki NAKAE　　Itaru HOSOMI　　Shunji ICHIYAMA
Human Media Res.Labs., NEC Corporation
{nakae, hosomi, ichiyama}@hml.cl.nec.co.jp

Abstract

This paper describes a billing and utilizing control system of a capsulated content in order to provide various services adaptable for its users' requests. Each element of a content is as well encrypted as so-called *super-disribution* systems. However, in this system, "Ticket-Keys" are generated from their each decryption key. Since each Ticket-Key depends on services provided by a capsule and its conditions in trading can be independently specified, if its users buy a "Ticket" for a particular service, then it can permit providing the service exclusively. With such a flexibility and security, its distribution is much promoted.

1　はじめに

PDF[1]やDigiBox[2]など従来のカプセル化コンテンツは，その設計時に利用目的や価格，再生環境などについて，非常に限定的な条件が課せられていた．例えば，高品質な画像の販売に際して，その利用目的として個人利用に限ったり，再生するPCの表示性能に最低限必要となる条件を設けたりといったことを余儀なくされていた．提供者の立場からはそれぞれの条件に合わせた単機能的なカプセル化コンテンツを複数流通させることで複数のサービスを提供することができるが，ユーザの立場からは別サービスのカプセルを改めて入手する必要があり，これはユーザにとって煩雑な作業でしかない．そこで，ユーザの要求に合わせて様々なサービスを提供しうるカプセル化コンテンツが望まれる．

そうしたカプセル化コンテンツの基本的なアーキテクチャとして，我々はすでにMediaShellカプセル化コンテンツを提案している[3]．MediaShellカプセル化コンテンツでは，構成要素データを個別に管理し，各データの出力制御をデータごとに行う．この際，ゲートキーパと呼ぶ出力制御機構により，後に述べるチケット受信や暗号化データの復号が行われ，多くのユーザ要求に適合しうる多様なサービスの提供を可能としている．

本稿では，まずチケットを用いたサービス毎コンテンツ販売の概念と利点について述べ（2章），チケットによる出力制御方式の詳細について述べる（3章）．そして，MediaShellにおけるコンテンツ流通実験のために構築したカプセル化コンテンツ再生システムの構成やその利用イメージなどを説明し（4章），最後にまとめを行う（6章）．

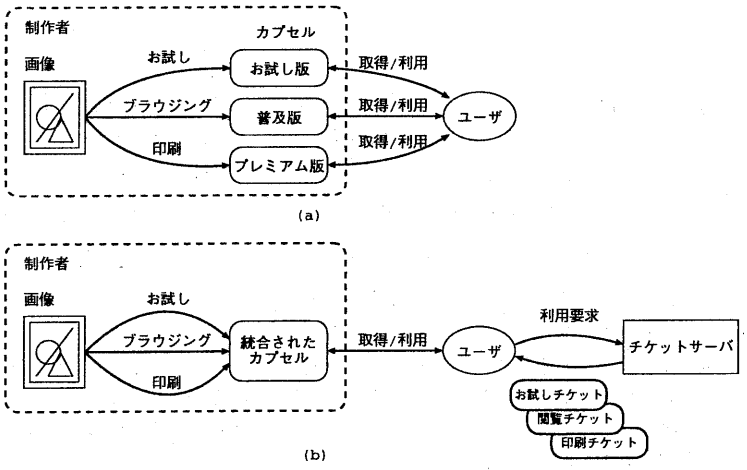


図 1: カプセル化コンテンツ流通形態の比較：(a) 従来型，(b) チケット利用

2 チケットを用いたコンテンツ販売

ここではカプセル化コンテンツのチケットを用いた各種サービスの販売について，そのコンセプトを例を用いて説明する．今，販売者が写真集や画集などいくつかの画像のアーカイブを販売するものとする．このアーカイブに含まれる各画像には，それぞれサムネール／ブラウジング用中精細／印刷用高精細の 3 種類が用意されていて，それぞれ「お試しサービス」「閲覧サービス」「印刷サービス」として異なる価格で販売することを考える．

従来のカプセル化技術によって，上記 3 種類のサービスを提供しようとした場合，サービス別に異なるカプセルとして配布し，それぞれの復号鍵をサービスに応じた価格で販売する方法がある．このとき，各サービスを順に利用したい場合，それぞれのパッケージを順に入手し，購入していく必要がある（図 1(a)）．これはユーザにとって煩雑な作業でしかない．

そこで 1 つのカプセルに複数のサービスを提供できるような手続きを持たせることで，1 度カプセルを取得した後はユーザの要求に応じたサービスを行えるようにすれば，別サービスを購入するために別カプセルを入手し，さらに復号鍵を購入する手間を省くことができる（図 1(b)）．こうしたコンテンツ販売方法は，コンテンツそのものを販売するのではなく，コンテンツに対するサービス利用権を販売するものといえる．

MediaShell カプセル化コンテンツでは，このようなサービス利用権に対して後述する「チケット」と呼ぶ実体を与え，これを取引することで利用権販売をわかりやすいものにしている．ここで，MediaShell における「サービス」は，

1. 許可される利用法：閲覧，印刷，保存など．
2. 構成要素データの集合：画像のみ/1 ページ/まるごと など．
3. 構成要素データに加えられる変換手続き：減色/解像度変換/電子透かし など．品質の制御に用いられる．
4. 課金額：数値＋通貨単位．
5. 課金方法：ペイパービュー/買取/回数限定 など．

の組により規定される．

サービス内容の提示については，コンテンツ制作者によってコンテンツの内容や用意したサービスに応じた適切な UI が提供される．例えば，初期画面でプルダウンメニューを用いてあらかじめ用意されたサービスをユーザに選んでもらう方法や，構成要素ごとにポップアップメニューを用いて随時サービスを選択してもらう方法などが考えられる．

MediaShell ではさらに，サービス内容およびそれを提供できる条件を定義するための ACL と呼ぶスクリプトを，カプセルとは別にチケットサーバで管理している．そして，ユーザからの利用要求があったとき，サービス提供の可否をチケットサーバで判断し，提供可能であればそのサービスに対応するチケットを発行する．このチケットが得られて初めて，カプセルは当該サービスの提供を行うようにしている（図 2）．

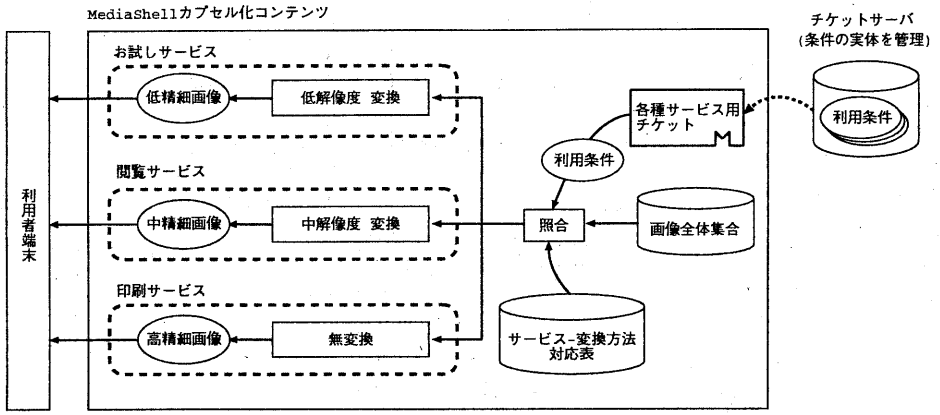


図 2: MediaShell におけるサービスの提供

こうすることでサービス内容や条件をカプセル配布後でも，カプセルに同梱した構成要素データの種類やデータ変換手続きなどの組み合わせの範囲内で，変更/追加することができる．例えば，印刷サービスが思うように売れない場合に，印刷用データに電子透かしを加えた上で保存を行えるようなサービスを追加するなどといったことが可能になる．こうして従来型の超流通システムでは困難であった，一旦配布された後のカプセルに対する利用制御ロジックの変更をある程度柔軟に行うことができる．このような特徴により，コンテンツ制作者はいつでも消費者ニーズに適合したサービスを提供できる機会をもつことになる．

3 チケット方式による利用制御

3.1 MediaShell カプセル化コンテンツ

MediaShell におけるカプセル化コンテンツのアーキテクチャは次のようになっている．シナリオやページ構造などを管理し，適応化表示機構を持つコンテンツマネージャと，コンテンツの各構成要素に対して利用認証や減色フィルタなどの出力制御を行うゲートキーパおよび暗号か構成要素データの組の集合から成る（図 3）．

ゲートキーパは図 4に示したような内部構成をもち，暗号化構成要素データの復号に際してチケットサーバを介した利用認証と，利用法に応じたデータ変換を行う．この動作の詳細を以下に述べる．

まず，コンテンツマネージャよりデータの出力要求を受けたゲートキーパは，通信制御部を介してチケットサーバよりチケットを発行するよう依頼する．このとき，チケットサーバに伝えるメッセージの内容は以下の通り

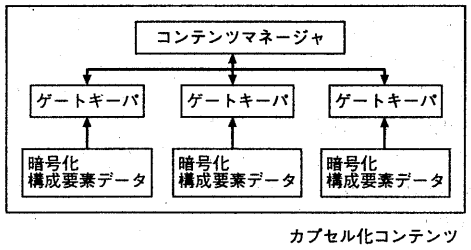


図 3: カプセル化コンテンツの基本構成

である．

- 要求元ユーザ名
- 要求元ホスト名
- コンテンツ名
- ゲートキーパ ID
- サービス ID/ユーザ側提示条件
- 要求年月日
- 要求元ユーザによるデジタル署名

チケットサーバはゲートキーパとの通信制御モジュール，利用条件記述（ACL）のデータベース，チケット発行可否を判断するための ACL 解釈部とから構成されている．チケット要求を受けたチケットサーバはデータベースから適切な ACL を検索し，ACL 解釈部において当該 ACL を参照しながら，上記メッセージ中の要求元

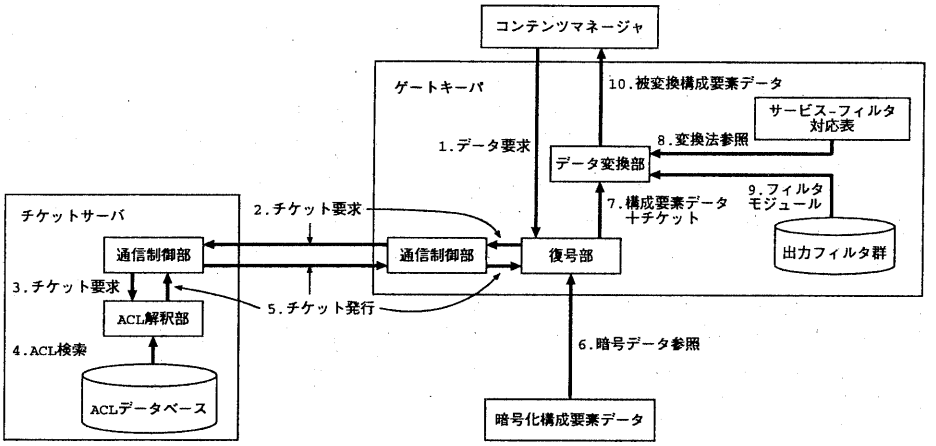


図 4: ゲートキーパおよびチケットサーバの内部構成

ユーザ名/利用法/端末能力などのユーザ側提示条件と，ACL 中の利用条件とを照合する．照合した結果，要求を受理する場合，以下のようなフォーマットをもつチケットを生成し，要求元のゲートキーパに返す．ただし，その際，チケットは要求元ユーザの公開鍵証明書に含まれる公開鍵により暗号化され，第三者による不正入手から保護される．

- 要求元ユーザ名
- 要求元ホスト名
- チケットサーバホスト名
- コンテンツ名
- ゲートキーパ ID
- サービス ID/利用時制約条件
- チケット鍵
- 課金額/課金方法
- チケット発行年月日
- チケットサーバによるデジタル署名

こうして発行されたチケットを受け取ったゲートキーパは，復号部でチケットに記されたデジタル署名を確認し，チケット鍵を参照して，後述するような復号化処理に基づいて暗号化構成要素データを復号する．復号された構成要素データは，データ変換部において，サービス-フィルタ対応表とチケットに記されたサービス ID/利用時制約条件とを照合して，必要な変換フィルタとそのパラメータを決定する．そして，その変換フィルタをゲートキーパ内に保持された変換フィルタ群より抽出し適用する．こうしてサービスに基づいて適切な形に変換されたデータはコンテンツマネージャに渡され，ユーザに提示される．

3.2 チケット方式の詳細

カプセル化コンテンツ内で，各ゲートキーパが持つ構成要素データは，それぞれ異なる鍵を用いて対称鍵暗号により暗号化されている．今，各構成要素データを $D_1, D_2, \ldots, D_n$ とし，各データに対する鍵を $K_1, K_2, \ldots, K_n$ とする．このとき，各ゲートキーパが持つ暗号化構成要素データを次のように書く．

$$\begin{aligned} ED_1 &= \{D_1\}^{K_1}, \\ ED_2 &= \{D_2\}^{K_2}, \\ &\vdots \\ ED_n &= \{D_n\}^{K_n} \end{aligned}$$

このとき，鍵 K_i から次のような値 TK_i^{UK} を算出する．UK はある特定の構成要素データについて，あるサービスに一対一対応する数値であり，利用鍵と呼んでいる．

$$\begin{aligned} TK_i^{UK} &= \{K_i\}^{UK} \\ UK &= \mathrm{hash}(spec(ED_i, service)) \end{aligned}$$

ここで，$spec(ED_i, service)$ は，“コンテンツ名 | 著作者名 | 構成要素 ID| サービス ID” として表される．

各暗号化構成要素データ ED_i はカプセルに同梱され，ED_i およびサービスごとのチケット鍵 TK_i^{UK} は ACL

内に記述されチケットサーバで管理される．MediaShellにおいて，チケットサーバは信頼できる第三者として機能する．

次に暗号化構成要素データの復号について説明する．前節でも述べたように，任意のある時点で，必要な構成要素データについてユーザからサービスが指定され，対応するチケットを取得した後，構成要素データの復号および出力が行われる．この手続きを形式的に示すと以下の通りとなる．

$$(1)\quad UK = \mathrm{hash}(spec(ED_i, service))$$
$$(2)\quad K_i = \{TK_i^{UK}\}^{UK}$$
$$(3)\quad D_i = \{ED_i\}^{K_i}$$

以上のようにして，本方式ではそれぞれの構成要素データに対して，サービスに応じて異なるチケット鍵を生成し，チケットに記録して配送する．もし単に復号鍵を記録する場合，復号鍵を取り出して不正に構成要素データを入手しやすいのに比べて，本方式ではチケットに復号鍵が直接記録されないので，そういった安易な不正を防止できる．安全性についてのより詳しい議論は，5.1節で述べる．

3.3 ACL

電子的著作権管理システム（ECMS）やコピーマート研究に関連して，利用条件や課金条件などを含めた権利記述を形式的に表し，データベースを用いて管理／運用していこうという研究が盛んである．最近では，星野らによって，利用形態や改変時の条件など複合的な条件を記述しうるXMLベースの権利記述が提案されていたり[4]，RDFを応用して，二次的著作における著作者間の権利関係を記述しようとする研究[5]もある．

本研究でも，このような高機能な利用／課金条件の記述を目標としているが，現在チケット方式に必要な情報だけにとどめている．ACLでは，各コンテンツごとに，(1) 構成要素ID，(2) サービスID，(3) 利用/課金条件およびチケット鍵，の順に構造的に記述している．例えば，

```
picture1 {                          #構成要素名
  RegularView {                     #サービスID(通常閲覧)
    cond {                          #利用条件
      Resolution <= 640x480         #解像度の上限
      ColorDepth <= 16              #色数の上限
      Price = 30                    #課金額
      PaymentWay = PayPerView       #課金方法
    }
    key {                           #チケット鍵定義
      9AFB38A235A0FC89
    }
  }
  PremiumView {                     #サービスID(プレミアム閲覧)
  ...
  }
}
```

といったように記述される．この例において，構成要素picture1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ビットとする．課金額は30円で，課金方法はペイパービューである．」と解釈される．

4 カプセル化コンテンツ再生システムの構築

4.1 システム構成

以上までで述べたようなチケット方式による利用制御機構を備えたカプセル化コンテンツの再生環境を試作した．本システムでは，コンテンツとしてWebページを対象とし，一般的なWebブラウザ（以下ブラウザ）をもちいて再生環境を構築した．本システムの構成は図5の通りである．

図からわかる通り，ローカルプロキシが本システムの中心となる．ローカルプロキシは(1)一般的なHTTPプロキシ機能と，(2)カプセル化コンテンツに再生データを要求し，取得したデータをブラウザに返すカプセル化コンテンツ再生機能とを持つ．このような構成にすることで，一般的なブラウザをカプセル化コンテンツビューワとして動作させることができる．

4.2 システム概要

今回，当研究所の作成のマルチメディアコンテンツ「道」[6]を実験的にWeb化し，カプセル化したものを用いた．「道」は京街道沿いの風景写真が主な要素であり，風景にちなんだ伝承・逸話を写真とともに閲覧できるようになっている．今回，以下のような仮定を設定し，カプセル化を行った．

- 提供するサービスとして，プレミアム版・廉価版・お試し版の3種を用意する．—「コンテンツ松竹梅」
- 利用制御の対象（=課金の対象）は，各写真のみとし，課金方法を一律ペイパービューとする．
- 決済システムとしてICカードによるプリペイドカードを用いる．
- ICカードはあらかじめ松竹梅に対応した3種のカードが発行されるものとする．したがって，サービスの選択は閲覧時に挿入されたカードの種類に従う．

4.3 利用制御および課金の様子

本システムの動作について説明する．

まず，ユーザはブラウザおよびローカルプロキシを立ち上げる．ブラウザのオプション設定により，プロキシサーバとしてローカルプロキシ（localhost:8080）を指

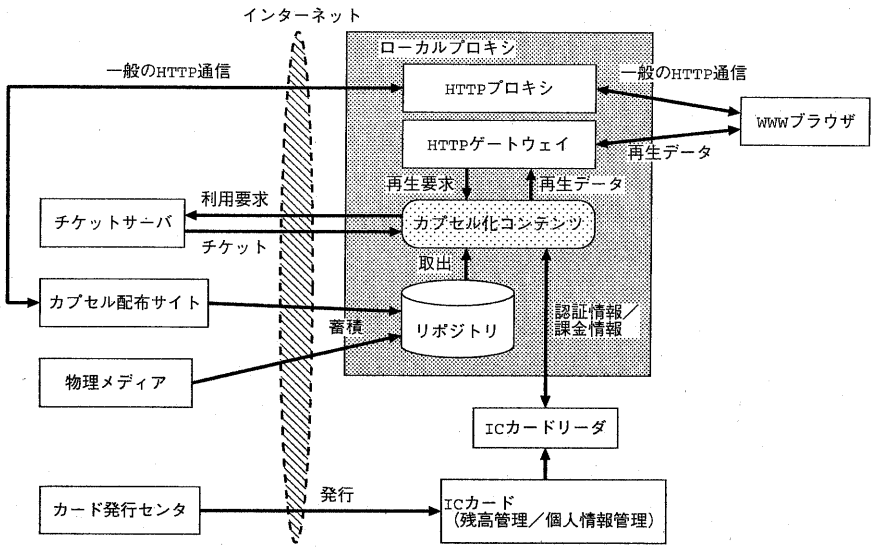


図 5: カプセル化コンテンツ再生システム構成

定する．また，ローカルプロキシの 9090 番ポートをプロキシ例外として指定する．

次にユーザはカプセル化コンテンツを入手しなければならない．本システムでは,「リポジトリ」と呼ぶ特定のディレクトリにカプセル（.msh ファイル）を置くだけで良い．したがって，フロッピーディスクや CD-ROM で配布される場合は，カプセルをリポジトリにコピーし，ftp などを経由する場合はリポジトリをダウンロード先として指定すればよい．

本システムでは，特に HTTP 経由での配布に便宜を図っている．これは，カプセル化コンテンツのサービス内容や価格体系などの説明に関して訴求力の高い配布サイトを構築する上で，WWW の利用が最も期待されるためである．配布サイト上で，ユーザがあるカプセル化コンテンツを選択したとき，WWW サーバはカプセルのダウンロードを開始するが，ローカルプロキシはそれを自動的に検知しリポジトリに格納する．その後，直ちにカプセルからタイトルページを取り出し，9090 番ポートを通じてブラウザに表示する（図 6）．この間の動作はユーザから透過的であり，入手したものが直ちに再生されることで，ユーザにとっての簡便さとわかりやすさを実現している．

前節でも述べたように，本システムでは「コンテンツ松竹梅」なる品質別の閲覧サービスを行えるようにしている．IC カードにはあらかじめ松カード／竹カードの

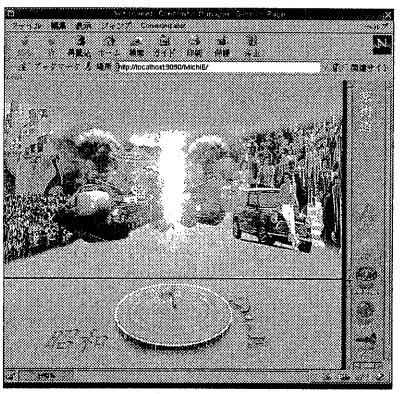


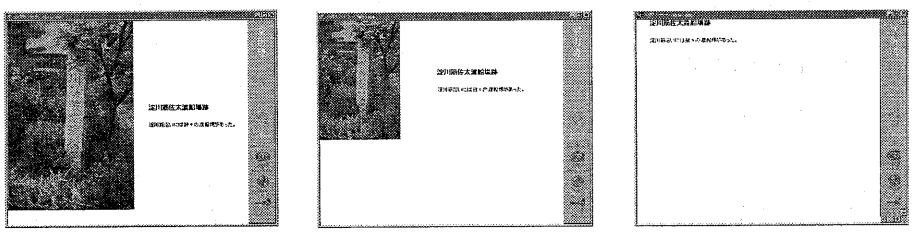
図 6: 試作コンテンツのオープニング画面

2 種類が用意されており，それぞれ「松」コース／「竹」コースに対応している．また，IC カードが無い場合は，自動的に「梅」コースが選択される．それぞれのコースの画面表示例を図 7に示す．

5 考察

5.1 安全性

前章までで，チケットや IC カード利用によるユーザや著作者の便益について説明した．ここでは，MediaShell



松　　竹　　梅

高解像度・フルカラー写真つき　低解像度・モノクロ写真つき　写真なし（無料）

図 7: 閲覧サービス 3 種（例）—写真提供：外山達志

におけるデジタルコンテンツの不正利用に対する安全性について議論する．

チケットを用いたカプセル化コンテンツ流通において考えられる不正は様々であるが，次のように大別することができる．

1. ユーザもしくは第三者による暗号化構成要素データの解析
2. 第三者によるチケットの窃取
3. ユーザによるチケットの他サービスへの不正転用
4. ユーザによる第三者へのチケットの不正頒布

まず，1番目の不正については，構成要素データを鍵長 128 ビットの Blowfish[7] を用いて暗号化することで保護している．このレベルの暗号は非常に安全であり，文献 [7] に示された見積もりに従えば，DES を平均 2 分で解読できるような力ずく攻撃専用ハードウェアを用いても，暗号化構成要素データの解読には平均的に 10^{16} 年かかる計算となる．

2番目の不正については，3章で述べたように，チケットをユーザの公開鍵で暗号化することで，たとえ第三者によりチケットが窃取されてもユーザの秘密鍵を知らない限り利用することができない．

3番目の不正については，チケット鍵は復号鍵そのものではないので，一般的なユーザによって単純に転用されることは考えにくい．ただし，十分なスキルを持つユーザであれば，ゲートキーパの動作をトレースしたり，3章で述べた方法を模倣することも不可能ではない．トレースについては，データフローの撹乱を行う Obfuscation 技術を適用することでトレースを非常に困難にさせることができる。一方、復号鍵の不正な復元については、今後利用鍵の生成方式をより高度なものにすることで対処できると考えている．

最後に 4 番目の不正については，チケットを各ユーザ別に公開鍵暗号化した上で配布しているので，第三者にチケットを渡す場合は (1) 自身の秘密鍵を添えるか，(2) チケットを復号した上で第三者の公開鍵により暗号化して渡すか、のどちらかの方法をとる必要がある。前者のような不正は技術的には容易ではあるが、ネットワーク上での身元証明である秘密鍵を渡すようなことは非現実的である。一方、後者のような不正はある程度のスキルが必要ではあるが、実行しやすい不正といえる。現在、このような行為を防ぐことはできないが、IC カードに秘密鍵を記録し、そのアクセス権を適切に設定することで困難なものにすることができると考えている。また，チケットは一つの構成要素データに対してのみ有効であり，万一チケットが不正に頒布されても，その被害はただ 1 つの写真データなどに過ぎず，経済的な被害は最小限で済む．こうしたことも MediaShell カプセル化コンテンツの特長の一つである．

5.2 デジタルコンテンツの事業性と公益性

前章までで説明したチケットを用いたサービス毎コンテンツ販売方式は，徹底されたライセンス販売方式といえる．近年の米国における UCC2B 関連の議論 [8] にもあるように，「学術と有益な技術の発展の促進」という言葉で表現される公益性と，デジタルコンテンツをビジネスの対象とするための事業性とのバランスの問題がある．こういった意味で，チケット方式はいくぶんビジネスに片寄ったアプローチといえる．

しかし，この問題を以下のような小問題に還元できるならば，チケット方式は両者のバランス取りに貢献できると考えている．

- 個人利用／学術利用の自由
  - 限定的条件下での複製
  - 個人的なライセンス譲渡
  - 引用
- コンテンツ創作の促進
  - 二次的著作と二次的著作者の利益確保
  - 流通の仲介者の利益確保

まず，個人利用／学術利用の自由についてであるが，デジタルコンテンツの特性により，事業性の確保という立場から，複製の自由は認められるものではない．しかし，個人的なライセンス譲渡や引用に関しては，チケットの譲渡が行えるようにするなどといったチケット方式の改良により対応できると考えている．

次に，コンテンツ創作の促進についてであるが，二次的著作の実現が必須と考えている．これはデジタルコンテンツのリテラシー普及が，文化への寄与と市場規模増大への寄与という両側面に対する効果が期待できるためである．この際，二次的著作物の権利記述と利用制御という2つの技術が必要になる．利用制御に関しては，現在，構成要素単位で権利者が異なる場合にのみ対応可能であるが，複数の権利者が同時に存在する要素オブジェクトの利用制御については未対応である．このような場合，複数の権利者それぞれにより発行されるチケットを全て集めてはじめて復号鍵を得ることの出来るようなチケット方式の改良を行えば，対応可能と考えている．一方，権利記述に関しては，権利関係の記述方法などについては先行技術の導入により解決できるだろうが，今後は一次／二次著作者間での権利交渉の支援がより重要な問題になるものと思われる．

また，今後，ポータルサイトや仮想店舗などコンテンツ流通の仲介者の役割が大きくなるものと思われ，仲介者の利益確保がより重要な課題となる．InterTrust の DigiBox[2] はこの点を考慮した機能をもつ．本研究においても，上記のような仲介者がチケットサーバの運営を担うものと考えており，チケットサーバ運営者によるサービス付加と利益分配を可能にする技術の開発を進めていきたいと考えている．

6 おわりに

以上，デジタルコンテンツ流通基盤 MediaShell における，ユーザの多様な要求に適合しうる種々のサービスを提供するためのチケットを用いたコンテンツ販売について説明した．

また，そのようなビジネスモデルを実現するためのカプセル化コンテンツアーキテクチャ，特にチケットによる利用制御方式と利用条件記述について説明し，さらにその実証のため，ローカルプロキシを中心としたカプセル化コンテンツ再生システムを構築したことを説明した．

最後に，チケット方式の安全性について議論すると共に，デジタルコンテンツのもつ事業性と公益性のバランス適正化という観点から本方式の今後の在り方について考察し，(1) 個人的/学術的利用の限定的自由を確保すること，(2) 二次的著作物の作成と流通を可能とすること，(3) 店舗など仲介者の利益を確保すること，などの重要性について述べた．

参考文献

[1] Adobe Inc., "Portable Document Format Reference Manual Version 1.2", **http://www.adobe.com/supportservice/devrelations/PDFS/TN/PDFSPEC.PDF**.

[2] Olin Sibert, et al., "Securing the Content, Not the Wire, for Information Commerce", **http://www.intertrust.com/secure-the-content.html**.

[3] 細見他，"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"，情処研報，Vol. 98, No. 85, EIP-2, pp. 49–56, 1998.

[4] 星野他，"コンテンツの複合的権利記述による権利保護と流通支援"，情処研報，Vol. 98, No. 85, EIP-2, pp. 1–8, 1998.

[5] 熊沢他，"多権利者間の権利関係の記述によるコンテンツ再利用支援"，第57回情処全国大会 (分冊4), pp. 232–233, 1998.

[6] 野田他，"時空間の視覚化手法～年輪メタファを組み込んだ時空間ブラウジングコンテンツ～"，インタラクション '98, pp. 135–136, 1998.

[7] B. Schneier, *Applied Cryptography 2nd Ed.*, Wiley, 1996.

[8] P. Samuelson, "Does Information Really Have to be Licensed?", *Comm. ACM*, Vol. 4, No.9, Sep. 1998.