

視聴率による利益分配型コンテンツ流通方式の提案

藤井 治彦 塩野入 理

日本電信電話株式会社 NTT 情報流通プラットフォーム研究所

{fujii.haruhiko, shionoiri.osamu}@lab.ntt.co.jp

従来のコンテンツ流通方式は、CD→無著作権保護方式→P2Pというパターンには、全く対処ができなかった。また、コンテンツにどのような不正コピー対策をしても、いずれコピープロテクトが解かれP2Pで出回ってしまう。更に大きな問題は、無料の無著作権保護方式やP2Pは、非常に利便性が高いため、圧倒的なユーザの支持があることである。本方式では、コンテンツを一般道路や図書館のような共有財産とみなし、全て使い放題かつコピーフリーとする代わりに、ユーザは利用量に関係なく定額料金を支払う。管理サーバは再生ソフトから使用記録を集計して視聴率を作成し、これに応じて報酬を各クリエイタに分配する。本方式を用いれば、無著作権保護方式と同等の利便性が得られ、不正コピーはなくなる。また、P2Pとも共生も可能であり、不正コピーされたコンテンツのクリエイタに対しても、想定される利用量に応じた正当な報酬が分配できる。

A new content distribution method utilizing popularity figures that can reward content creators appropriately

Haruhiko FUJII and Osamu SHIONOIRI

NTT Information Sharing Platform Laboratories, NTT Corporation

The conventional content distribution method cannot prevent illegal peer-to-peer (P2P) sharing of non-copy-protected data on compact disks (CDs). And any copy protection scheme will soon be analyzed, and the content data will be shared among many people by P2P. Almost all users like free non-copy-protection methods because of their convenience. Our method regards all contents as collective property. So users are free to make copies and are not metered for usage, but are charged a flat rate. The control server tracks usage and generates popularity figures from the player software on the user's computer, and distributes appropriate rewards based on the popularity of the content. This method gives users usability comparable to non-copy-protection methods, so if enough people use our method, the flat-rate fee become reasonably low and there will be no economical motivation for illegal copying. And it is compatible with any P2P scheme, and can distribute rewards corresponding to the estimated amount of usage to creators whose content has been illegally copied.

1. はじめに

これまでに様々なコンテンツ流通方式が提案されてきたが、無著作権保護方式に比べ、私的コピー、ファイル交換、バックアップなど様々な面でユーザの利便性を制限しており、ユーザの支持を得ていない^{1,2}。また、Peer-to-Peer (以下、P2Pと略記)による不正コピーを摘発するために、ネット上を流通するファイルをフィルタリングして個々のユーザを告発するという案も出てきているが、実効性やプライバシーの問題は未解決である。

実際に、ノンパッケージ配信の伸びに比べて、P2P ファイル共有ソフトによる無料ファイル交換の数は急増している³。逆に、映画、CD、書籍、新聞などパッケージコンテンツは全て減少傾向にあるが⁴、これは、無料のWEBニュース、無料の楽曲などの発展が原因と考えられる。ブロードバンド化や通信費の低額化を考えると、この問題は加速するであろう。この状況が続けば、クリエイタの報酬は激減し、コンテンツのレベルが落ち、ひいてはユーザが不利益をこうむることになる。

本稿では、不正コピー問題の大きさや根絶が難しいことを示し、現行のコンテンツ流通方式が成立困難であることを示した後、これを打開する、クリエイタの競争原理とユーザの利便性を保ちつつ、クリエイタに正当な報酬を確保できる、コンテンツ流通方式を提案する。

本方式の特徴は、過去に不正コピーされてしまったコンテンツに対しても、クリエイタに正当な報酬が分配される点であり、この点は、他のコンテンツ流通方式では実現できなかった。また、無著作権保護方式と同等の利便性があり、P2Pとも

共生が可能である。更に、ストリーミング/ダウンロードを問わず、どんなノンパッケージコンテンツに対しても本方式を適用できる。

2. 現状の問題点

現状の問題点は、大きく分けて2つあると考える。それは、P2Pなどの技術革新により、不正コピーは防げなくなるといふ「不正コピー問題」と、不正コピー問題がなかったとしても、従来の著作権保護方式などによっておこる利便性の低さなどの「従来方式の問題」である。

2.1. 不正コピー問題

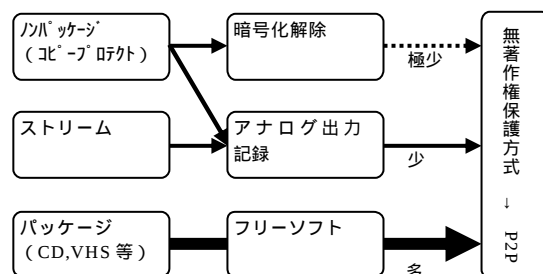


図 1 不正コピーファイルの出元

図1に示すように、不正コピーは、パッケージコンテンツからのコピーが大半であり、CD、VHS や DVD は、フリーソフトなどで簡単にHDDにコピーが可能である。ユーザは、このファイルをNapster⁵やGnutella⁶に代表されるP2Pファイル共有ソフトを介して不正流通させている。

不正コピー問題には、P2Pの急速な発達という技術的な問題と、不正コピーコストの低下というコスト面からの問題と、法律的問題がある。

2.1.1 P2Pの急速な発達

デジタル白書⁴によると、CDの生産金額は2000年で5200億円であり、2年連続で前年度割れとなった。代わりにNapsterによる国内の被害総額は2001年5月現在で、143億円になっている³。CD業界の生産額の落ち込みと不正コピー額の増加には、明確な因果関係は証明されていないが、不正コピーの被害総額は、今後飛躍的に伸びると考えられる。先に述べた被害総額はNapster単体のものであり、現在は、有名なものだけでも表1のような同種のソフトがある。

表1 代表的なP2P ファイル交換ソフト

技術名	2001年8月の一ヶ月間に、米国でダウンロードされたファイル数
ファーストラック	9億7000万
オーディオギャラリー	9億1000万
アイメッシュ	6億4000万
グヌーテラ	5億3000万
合計	30億5000万
最盛期のNapster	30億弱

特に注目すべきは、ファーストラックの成長率が、60%/月であることと、取り扱えるコンテンツが、楽曲のみならず、映像、ソフトウェアであることである。更にP2Pの分野は、各企業が研究しており、SUNのJXTA⁵など、今後更に発達していくと思われる。

ブロードバンド化が、まだ進んでいない日本においても、Napsterのユーザ数は既に81万7千人に達しており(2001年5月現在)、これは全インターネット人口の4.4%に相当する³。このユーザ数はNapster以外のP2Pファイル共有ソフト全体だと、更に多くなるであろう。また、マスコミにP2Pが紹介される回数も増えており、これによりユーザ数が増え、また、マスコミに紹介されるという悪循環があり、一部のユーザの間では、音楽でさえインターネットのコンテンツは無料であるという認識が広まっている。

2.1.2 不正コピーコストの低下

ネットワークのブロードバンド化や低価格化は、不正コピーのコストを大幅に下げた。従来は、不正コピーは一見無料で手に入るように思えるが、実際は通信コストがかかるため、正當に購入したほうが安い場合があり、これが不正コピーの流行を抑えていた。例えば、一昔前であれば、ダイヤルアップ(伝送容量56kbps、実行スループット25%)で、5分の楽曲(サンプリングレート128kbps)をダウンロードすると、所要時間は約45分であり、この電話料金(3分10円)は150円、プロバイダ料金(1分10円)は450円となり、不正コピーコスト

は合計600円となる。これでは、レンタルCD店に実際に出向いて借りてくるほうが、安いこととなり、不正コピーは、あまり意味がなかった。

しかし、現在は、ADSLやFTTHが普及しだしており、低価格かつ短時間の内に、多くの楽曲をダウンロードすることができる。また、データ量が大きくて不正コピー困難な映画やソフトウェアも、FTTH時代には、すぐに手に入るようになると思われる。

2.1.3 P2Pの法的解決の困難さ

P2Pは、Napsterのような中央サーバを持つHybridP2PとGnutellaのような中央サーバが不要なPureP2Pに分類が可能である。訴訟が有効なのは、HybridP2Pである。なぜならば、このタイプは、中央サーバの管理者(管理会社)さえ、訴訟などをおこして営業を停止させればシステム全体が停止するからである。しかし、このような訴訟による手法もあまり期待できない。なぜなら、訴訟には多大なコストがかかり、このコストは最終的にはコンテンツの値段に跳ね返るからである。また、一つの業者を訴えても、すぐに次の業者が現れる。またサーバを外国に置くなどすると、法的解釈はさらに困難になる。また、裁判に仮に2年かかるとしたら、その間にユーザ数を、増やすことができるし、またノーティス・アンド・テークダウン⁶を使用する業者もいる。

PureP2Pでは、訴訟による解決は更に困難となる。なぜなら完全な分散システムなので、システムをとめるには、一人ずつユーザを告訴していくしかなく、これは、ユーザの猛反発を受ける可能性が高い。また、ネット上を交換されるファイルを監視するというものの提案されているが、これは、プライバシーの問題もあるし、リネームするなどして容易にすり抜けることが可能である。

2.2. 従来方式の問題点

表2に示すように、オンライン配信のための新しい技術やビジネスモデルが、たくさん提案されている¹⁰が、それぞれ課題を抱えている。また、どれも無料P2Pにはかなわない。

この他にも、Napsterは、課金処理機能をつけたりしたが、ユーザ数が急減(36%減)し、それらのユーザは、他の無料P2Pへ移動しただけであった¹¹。

また、各方式間での著作権保護システムや記憶媒体の互換性や課金システムの不統一性、モバイルの通信費の高さが問題となっている^{1,4}。たった数百円のコンテンツを購入するために、クレジットカード番号やその他の個人情報が必要であり、利便性の面からも、個人情報保護の面からも課題があった¹。この意味では、P2Pはユーザ登録が不要であるので、プライバシーの問題がないともいえる。

また、従来方式は、ハッキングの脅威に常にさらされているわけであるが、最近の米国の判決例では、ハッキングソフト

* ファーストラックを利用した業者3社が2001年10月31日、全米レコード協会(RIAA)、米映画協会(MPAA)から著作権法違反の疑いで提訴されている。

† 著作権者からの一定の要件を備えた通知を受けた場合、速やかに検索リストから各コンテンツを削除することをISPに求める方式

を公開することは言論の自由とした判決もあり、更に問題を複雑化することが予想される。

表 2 技術/ビジネスモデルの分類と課題

大分類	要素技術	問題点
不正 コピー防止	暗号 特殊ハード	専用ハードが必要、利便性が低い。
	暗号 汎用ハード	ソフトウェアベースでの暗号化なので、暗号強度が弱い
不正 コピー抑止	電子透かし ネットウォッチ	抑止のみなので実効性が低い。プライバシーの問題。
不正 コピー許容 ^{12,10}	広告収入	不正コピーされたり確実な収入が望めない。インディーズが中心となっている。
	関連サービス	
	利用情報収集	
	チップ制	概念レベルの域をでていない。
	超流通 ²¹	
	OPIMA ¹³	

3. 提案方式

3.1. 提案方式の概要

2 章で説明したように、従来のようなコンテンツ流通方式は非常に成立困難であるといえる。もし、従来方式を成立させていけば、教育などによって、ユーザのモラルに頼るしかないか、もしくは、ネットワッチの強化や PC のようなオープンなプラットフォームの回収などしかないと考えられる。しかし、これらは実現するのに多大な時間と労力を要するし、何よりも、技術の発展によって得られた利便性を、わざわざ制限しているので問題である。あるいは、従来方式を諦めると現在の多くの個人のホームページやフリーソフトのようにコンテンツのクリエイタにボランティアを強要する情報社会主義¹⁴しかない。しかし、これでは市場原理・競争原理が働かず、コンテンツの質の向上が望めない。ただし Linux のような例外もあるが、一般のコンテンツに対しては情報社会主義は適用困難である¹⁴。

よって、従来のコンテンツ流通方式とは、全く異なった方式を考える必要がある。

提案方式では、コンテンツを一般道路や図書館のような共有財産とみなし、使い放題、コピーフリーとすることによって、ユーザの利便性を確保し、代わりに利用率に関係なく一定に強制的に課金され、視聴率によってクリエイタの報酬を分配することにより、不正コピーを無意味化し、競争原理の元にクリエイタの報酬を確保し、過去に不正コピーされたコンテンツも、その想定される利用量に相当した報酬を分配できるコンテンツ流通方式を提案する。

これにより、今まで、コピープロテクトのため費やされてきた多くの労力と、利便性の低さをなくするとともに、完全に P2P と共生できるコンテンツ流通方式を提案する。

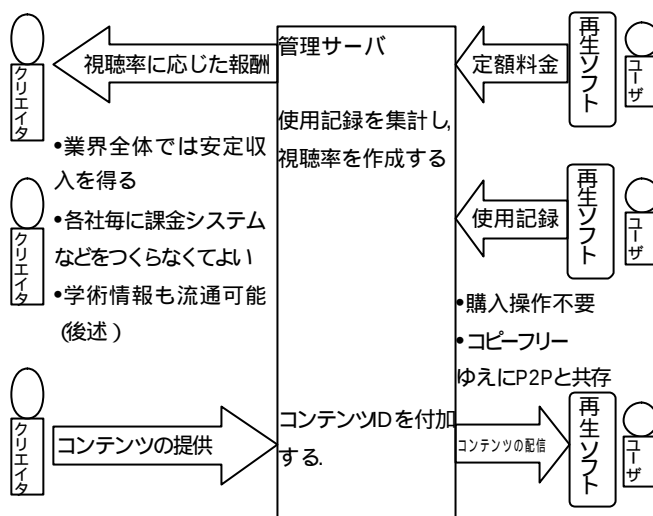


図 2 提案方式の原理

図 2 は、提案方式の概要を表した図である。構成要素としては、ユーザ、再生ソフト、クリエイタ、管理サーバがある。以下、各構成要素ごとに説明を行う

・ ユーザ

ユーザは、コンテンツの利用量に無関係に定額料金を支払う。従来方式では、コンテンツのダウンロードや再生ごとに課金されており、この部分を厳密に行わなければならない、システムの複雑化や利便性の低下を招いた。本方式では定額制とすることにより課金処理を独立させることができる。よってダウンロードごとにクレジットカード番号を入力する手間が省け、盗聴などによる個人情報の漏洩問題が緩和される。ただし、ユーザの定義として、コンテンツを視聴することができる全ての人を対象とする。

・ クリエイタ

クリエイタは、コンテンツにコンテンツID¹⁵をつけ、コピーフリーかつ無料でユーザに配布する。課金処理などが不要のため、P2P、C/S(クライアント/サーバ型)、メール、パッケージなど任意の経路でコンテンツを配布できる。また、ユーザもコンテンツを再配布してよい[†]。

・ 再生ソフト

再生ごとに使用記録を作り、月に一回などの割合で管理サーバに使用記録を送信する。ユーザは、複数の再生装置を所有できる。使用記録には、各コンテンツIDに対する再生時間などを記録する。

・ 管理サーバ

各再生ソフトから送信されてきた使用記録を集計して、視

* DVD の複製防止機構を回避するソフトである DeCCS の公開は、言論の自由であるという判決が、米カリフォルニア州高裁で出た。
http://www.zdnet.co.jp/news/0111/02/e_decss.html

† 著作権者は複製権と公衆送信権、著作隣接権者は送信可能化権を放棄する。現状ではネットワーク上での音楽著作物の使用料規定が決まっていないために多くのユーザ、事業者等が使用できずにいる状態にある。

聴率を算出し、クリエイタに報酬を分配する。

3.2. 提案方式の詳細

3.2.1. 課金方法

上記の方式では、コンテンツを視聴可能な全てのユーザが、必ず課金される必要がある。このようにすれば、不正コピーが成立しない。また、使用記録を書き換えてもユーザのメリットはないので超流通のように、使用記録の厳重な通信が不要になる。

理想的には、世界中の人が課金されることが望ましいが、受益者負担とするためには、年代別課金であるとか、PCや携帯電話やプロバイダ料に課金するという手法も考えられる。また、課金手法として税金を用いることも考えられる。

このような手法は、決して実現性がない手法ではない。例えば、一般道路やNHKのビジネスモデルが本方式に近いといえる。道路は税金の形で徴収されるが、一般道路は共有財産として無料で通行でき、また受益者負担としてガソリン税などが存在するし、NHKでは、見放題である代わりに、視聴可能者すなわちテレビを所有している者は、年数千円を定額で納めている。

3.2.2. 定額料金の目安

アメリカの有料P2P音楽交換サービス会社では、月5ドルの定額料金を課している¹⁶。また、インターネットユーザの内の成人の42%は、インターネット上の音楽に対してお金を払ってよいと考えている¹⁷。

実際に、本方式が完全に成立するモデルを想定して、月

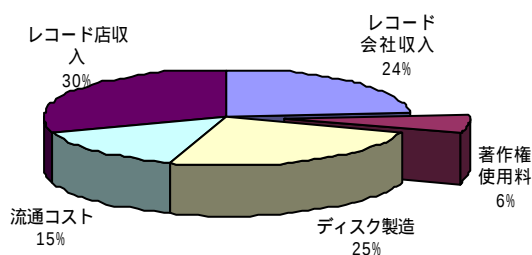


図 3：CD のコスト分布

額料金の概算を計算してみる。このモデルでは課金対象は、国民全員とし、中間業者の収益などを一切考えないものとする。

図3は、CDのコスト分布を示したものである¹⁸。CDの売上額うち、クリエイタの収入となるのは著作権使用料6%のみだと仮定する。現在のCDの売上高を5000億円とし、国民数を1億2000万人とすると、クリエイタに現在の収入を維持させるための、一月あたりの料金は、

$$5000 \text{ 億} \times 0.06 \div 1 \text{ 億} 2000 \text{ 万} \div 12 = 21 \text{ 円}$$

となる。さらに、表3に示すような他種のコンテンツ全てで同様のコスト構造、すなわち売上高に対する6%がクリエイタ業界に還元されると仮定すると、クリエイタ業界の収益を現状維持したまま、全ての国民が、表3に含まれる全てのコンテ

ンツを、ノンパッケージで使い放題になる月額料金は、

$$62000 \text{ 億} \times 0.06 \div 1 \text{ 億} 2000 \text{ 万} \div 12 = 258 \text{ 円}$$

となる。よって、月300円程度、年3600円程度さえ支払えば、国民は書籍・新聞を含む上表のコンテンツを再配布を含め、全く自由に使用することができる。また、本方式を用いれば、不正コピーなどにより、クリエイタの業界自体の収益が減ることではなく、競争原理も働くので、コンテンツの質は保たれる。ただし、このような方式が定着すれば、従来のパッケージコンテンツは成立困難になるという問題点もある。

表 3：パッケージコンテンツの売上高の目安^{4*}

種別	年間売上高の目安(億円)
出版	約 25000
新聞	約 25000
CD	約 5000
ビデオカセット	約 2000
DVD	約 1000
ビデオゲーム(ソフト)	約 4000
合計	約 62000

3.2.3. 視聴率集計方法

視聴率は、サーバ側で、ダウンロード数をもってカウントする方法も考えられる。しかし、コンテンツは再配布自由であり、ユーザからユーザへ流れていくので、ユーザ側でカウントするのが妥当である。また、逆にサーバ側でカウントする場合は、サイトごとに視聴率の偽造がないかどうかを証明せねばならず、また、個人放送局に対応するのも困難である。

3.2.4. 視聴率の定義と補正

例えば文章コンテンツや映像コンテンツの場合、単純な視聴率だけでクリエイタの報酬を決定するならば、低俗なものばかりが視聴率を稼ぎ、教養番組や論文など、視聴率は高くなくても社会的価値の高いコンテンツが不利益をこうむることが予想される。よって、コンテンツの種類に対して補正関数を施して調整することが望ましい。このようにすると、例えば論文などのように、従来、市場で流通困難だったコンテンツも、本方式では流通可能となり、研究者は論文で直接収入を得られるようになる。これは、従来から望まれていた論文の市場化を可能にするものでもある¹⁹。

ただし、補正関数はコンテンツごとに決定するのではなく、コンテンツの種類ごとに決定する。それにより、同種のコンテンツ内では正常な自由競争が働く。

表4表5に、補正関数の例と、コンテンツIDごとの補正值リスト、視聴率の算定例を示す。この情報は管理サーバ内にあり、両表を元に各コンテンツの補正関数を決定する。

● 視聴率の定義

視聴率は、相対的な再生時間から算出するものとする。また、これにユーザからの総収入をかけて各クリエイタへの分

* 地上波やBS・CS放送は元々ノンパッケージ流通であり、コスト構造や収益構造が大きく異なるため本考察には含めない。

配額を決定する。以下の数式 1 はコンテンツ ID が CID の視聴率の算定式である。

$$\text{数式 1} \quad \frac{T_{CID} \cdot X_{CID}}{\sum_{j=1}^N (T_j \cdot X_j)}$$

ただし、CID はコンテンツ ID、
N は総コンテンツ数
T は各コンテンツの累積再生時間
X は補正值

表 4：コンテンツの分類と補正関数の対応表

コンテンツの分類	補正值 (X)
一般娯楽	1.00
ニュース	2.00
教育 学術論文	3.00
猥褻 危険情報	0.10

表 5：コンテンツ ID と分類の対応表

コンテンツ ID (CID)	分類
1111111111	一般娯楽
2222222222	教育 学術
3333333333	ニュース
4444444444	一般娯楽
5555555555	一般娯楽

3.3. 提案方式のメリット

以下に、提案方式のメリットを整理する。

3.3.1. 競争原理下のクリエイターの報酬確保

本方式は、情報社会主義的に、クリエイタにボランティアを強要したり、コンテンツの視聴率に関係なく定額の給料制にしたりするものではない。また、現行方式のように不正コピーに対抗できずに業界全体の収益の減少を招くようなものでもない。視聴率による競争原理の下にクリエイタ業界の収益を確保できるので質の良いコンテンツを製作しつづける限り、クリエイタは良い報酬を確保でき、そうでないクリエイタは市場から退場を余儀なくされる。図 4 の実線は現在のクリエイタの収益分布図を示しており、提案方式は、これを維持できることを示している。

3.3.2. ユーザの利便性の確保

従来の著作権保護方式では、特殊なハードが必要であったり、コピー回数制限があったり、PC を買い換えと全てのコンテンツが再生できなくなったりした。また、ダウンロードごとにクレジットカード番号を入力する必要があったり、配信サイトごとにユーザ登録をせねばならず、個人情報保護の面からも問題があった¹。

また、逆に P2P は利便性や価格の面ではメリットがあったが、配信元が個人のため、コンテンツの品質の保証がなく、またダウンロード中に相手がネット接続を切ってしまう場合があった。

本方式では、コピーフリー 使い放題であり、配信経路も任意のものが取れる。またダウンロードごとの課金操作や、配信サイトごとのユーザ登録が不要である。

また、ベストヒットなどのコンテンツを集めて多数のクライア

ントに配信するような仲介業も、著作権者や管理サーバに特別な手続きをまったくする必要がなく成立が可能である。ただし、仲介業者は、現行方式のようにユーザからコンテンツ料金を請求するのは困難なので、広告を載せて収入を得るなどの副次的な収入を得なければならないであろう

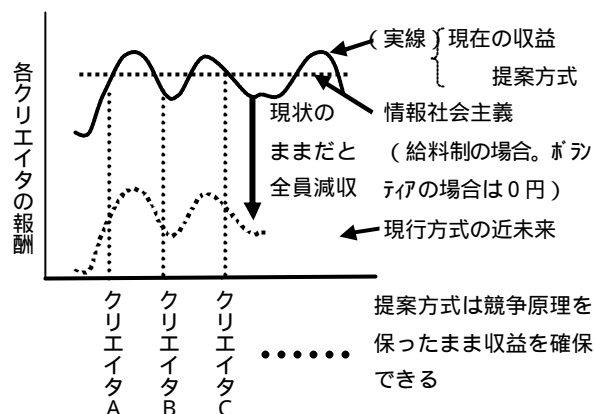


図 4 提案方式と現行方式と情報社会主義

3.3.3. 不正コピーされたコンテンツを正当に流通可能

本方式の大きな特徴の一つは、すでに不正コピーされてしまったコンテンツに対しても有効であるということである。これは、ある部分集合（本方式の対応のコンテンツ）の視聴率は、全体集合（不正コピーも含めた全コンテンツ）の視聴率と、ほぼ同じになる性質を利用したものである。よって、本方式の視聴率に応じて、全国民などから徴収した定額料金を分配すれば、不正コピーされたコンテンツも、使用量に応じた報酬が、クリエイタに対して還元されていることになる（図 5 参照）。

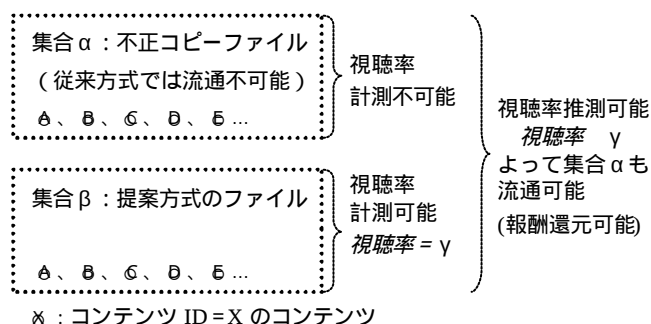


図 5 不正コピーファイルの流通の原理

3.3.4. 汎用性

本方式は、映像・ソフトウェアなど、コンテンツの種類によらず適用でき、また、非ダウンロードコンテンツ（ストリーム、WEB ページ）に対しても応用できる。また、特殊なハードなどが不要であるので汎用性が高い。

特に、補正関数の導入により、従来、市場化が困難であった論文のような特殊なコンテンツも流通を可能にした点である¹⁹。また、同時に、補正関数は、インターネット上のコンテンツの品質を向上させる効果もある。

3.4. 提案方式の課題

本方式は、あくまで理想的な方式であり、実現しようとした際には、以下に示す課題が発生すると考えられる。

3.4.1. クリエイタによる視聴率の操作

本方式では、コンテンツはコピーフリーかつ使い放題であり、ユーザはPCやプロバイダ料金に上乗せされるなどの手法で、予め強制的に料金を払うことになるので、ユーザの不正行為は、ほとんど発生しないといっても過言ではない。

しかし、本方式では、クリエイタの犯罪が起こる可能性がある。なぜならば、使用記録を操作することによって、自分の視聴率を上げることが可能であり、不正な収入を得ることが可能だからである。だが、従来のコンテンツ流通方式では犯罪の主体が不特定多数のユーザであったのに対し、本方式では、犯罪の主体は特定可能であり、極少数のクリエイタとなるので、問題はかなり改善されているといえる。

3.4.2. 実現性

本方式では、視聴可能な全てユーザが、強制的に課金されている必要がある。よって、理想的には、道路のように、国民全員から税金の形で徴収したり、PCや携帯電話やプロバイダ料金に課税する形が望ましい。インターネットの特性上、世界中の国で、本方式が実行されることが理想的であるが、実際問題として、このような解は難しい。

3.4.3. オフラインの再生ソフトには適用できない

使用記録を送信する必要があるため、本方式はオフラインの機器には適用できない。しかし、オフライン再生機器を除いても、全体の視聴率には、あまり大きな影響を与えない。また、最近は情報家電など、全ての機器がインターネットに接続する方向で動いているので、この問題は、さほど大きな障害とはならないと思われる。

3.4.4. 補正関数の決定

補正関数によって利益をこむクリエイタと、不利益をこむクリエイタが発生する。よって、補正関数の決定は、専門の第三者機関に委ねるのがよいであろう。

4. 部分集合モデル

4.1. 部分集合モデルの位置づけ

提案方式は、国民全体に課金するか、もしくはPCや携帯電話やインターネット接続料金に上乗せ課金する方式であるが、一度に実現するのが困難である。よって、より実現しやすいモデルを考察する。

部分集合モデルは、提案方式を擬似的に実現するモデルである。提案方式では、不正コピーには全く経済価値が発生しないことがメリットの一つであったが、部分集合モデルは、従来方式と同様、不正コピーは経済価値が発生する。しかし、国民全員が同時に提案方式を採用するというような、大きな前提条件を不要とし、一部の会員のみで実現が可能となる方式である。部分集合モデルの会員数が増加していくと、ス

ムーズに提案方式に移行できる。図6は、部分集合モデルと提案方式の関係を示したものである。

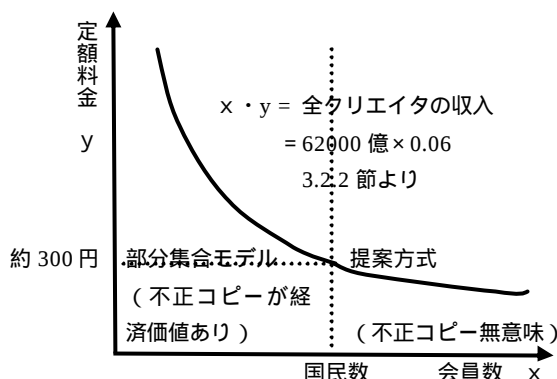


図6 提案方式と部分集合モデルの関係

4.2. 要求条件

以下に、部分集合モデルの要求条件を示す。

- (条件1) 会員ならば、コピーフリー 使い放題とする
- (条件2) 非会員は視聴できない
- (条件3) クリエイタには視聴率に応じた報酬が分配される
- (条件4) 定額料金を払わない会員は視聴できなくなる
- (条件5) 視聴率はクリエイタによって操作できない

4.3. 部分集合モデルの方式

図7は部分集合モデルの全体図を表したものである。部分集合モデルは、カプセル化、再生ソフトのインストール、配送、再生、視聴率作成 という5つの部分からなる。

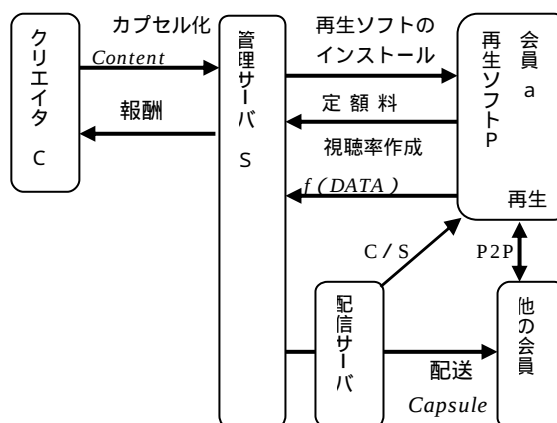


図7 部分集合モデルの全体図

以降、図7を用いて、各操作毎に詳細な説明を行う。なお以下の記号を使用する。

- K_s = 共通鍵方式の共通鍵 (コンテンツ暗号化用)
- K_D = 共通鍵方式の共通鍵 (使用記録暗号化用)
- K_{Ux} = 公開鍵方式のxの公開鍵 (Public Key)
- K_{Rx} = 公開鍵方式のxの秘密鍵 (Private Key)
- KU^n, KR^n = 使い捨ての公開/秘密鍵 (nは自然数)

- $EP[\text{key}, M], DP[\text{key}, M] =$ 公開鍵方式による暗 / 復号化(key は鍵, M は平文 / 暗号文)
- $EC[\text{key}, M], DC[\text{key}, M] =$ 共通鍵方式による暗 / 復号化(key は鍵, M は平文 / 暗号文)
- $\cdot$ = ビット列の結合
- $X\{I\} =$ X による I の署名。I に暗号化されたハッシュコードが附随しているものによって構成される。
- $P::X = P$ が X の処理を行う
- $P \rightarrow Q : M = P$ が Q にメッセージ M を送る
- その他

C = クリエイタ, S = 管理サーバ, P = 再生ソフト

Content = コンテンツ, Capsule = カプセルコンテンツ

CID = コンテンツID, SID = 再生ソフトのID

ID x = 会員 x の ID, DATA = 使用記録

4.3.1. カプセル化

サーバは、まず平文のコンテンツのカプセル化を行う。

- (1) $C \rightarrow S : \text{Content}$
- (2) $S::S\{EC[K_s, CID \quad \text{Content}]\}$ を作成し、Capsule とする

管理サーバの署名をするのは、コンテンツIDの書き換えをされていないことを証明するためである。

4.3.2. 再生ソフトのインストール

会員は、はじめに、再生装置 (ハード) に毎に、再生ソフトをインストールする必要がある。また、再生ソフトを識別するSIDは配信サーバSが発行する。

- (1) $S \rightarrow P : \text{インストールプログラム} \quad KU_s$
- (2) $P \rightarrow S : ID_a \quad KU_a$
- (3) $S::SID$ を発行し、表 6 の会員リストを更新する
- (4) $S \rightarrow P : EP[KU_a, K_s \quad SID \quad KU^0 \quad K_D]$

表 6: 会員リスト

会員 ID	最終入金日	SID	...
IDa	2001/10/4	11111	
		22222	
		33333	
IDb	2001/9/24	44444	

本方式では、 K_s, SID, KU^0, K_D のいずれかが、盗聴されると、カプセルコンテンツの不正復号や、使用記録の改ざん、成りすましが可能であるので、上記のような通信をおこなう⁰。また、ユーザは複数の再生装置 / 再生ソフトを所有することを想定している。

4.3.3. 配送

コンテンツの配送は Capsule を任意の経路で送る。また、配送時の課金処理も不要である。

4.3.4. 再生

使用記録 DATA は表 7 のフォーマットをとる。

使用記録は、 K_D で暗号化されて保存される。再生コマンドが入力されると、以下の手順で再生される。

- (1) $P::\text{Capsule}$ の署名を KU_s を用いてチェックする
- (2) $P::\text{Capsule}$ から $EC[K_s, CID \quad \text{Content}]$

を取り出す

- (3) $P::DC[K_s, EC[K_s, CID \quad \text{Content}]]$ より CID, Content を取り出す。
- (4) $P::\text{Content}$ の再生を行い、再生時間を記録する
- (5) $P::DC[K_D, EC[K_D, DATA]]$ より DATA を取り出す。
- (6) $P::\text{DATA}$ 中の各当するコンテンツIDの累積再生時間と合計再生時間に、今回の再生時間を加算する
- (7) $P::$ 合計累積再生時間が、規定値以上 (例えば 10 時間以上) ならば、再生機能をロックして、視聴率作成に進む
- (8) $P::EC[K_D, DATA]$

使用記録を暗号化するのは、会員が使用記録を改ざんできないようにするためである。また、使用記録には、各コンテンツIDが、累積で何秒再生されたかが記録されており、各コンテンツの累積再生時間を全て足し合わせた合計累積再生時間も記録されている。

表 7: 使用記録のフォーマット

コンテンツID	累積再生時間[sec]
1111111111	20
2222222222	300
3333333333	4000
合計累積再生時間	4320

4.3.5. 視聴率作成

本操作は、再生時間の合計が規定時間内 (例 10 時間) になるたびに行われる。また、本操作が初めて行われる場合は $n=0$ である。

- (1) $P::DC[K_D, EC[K_D, DATA]]$ より DATA を取り出す。
- (2) $P \rightarrow S : EP[KU^n, SID \quad DATA]$
- (3) $S::DP[KR^n, EP[KU^n, SID \quad DATA]]$ より SID と DATA を取り出す。
- (4) $S::$ 表 6 の会員リストを参照し、SID の所有者の最終入金日が一月以内かをチェックする
- (5) $S::$ 表 8 のフィルターをかける

表 8: フィルター

チェック項目
使用記録は 1000 分の 1 などの割合でランダムに選択し、残りは破棄する
特定の CID の再生時間が異常に長いものは破棄する
同一の SID から、規定時間以内 (例えば 10 時間以内など) に送られてきたら、破棄する

- (6) $S::$ フィルターを通った DATA を会員全体の使用記録にマージされる
- (7) $S::KU^{n+1}, KR^{n+1}$ を生成する
- (8) $S \rightarrow P : EP[KR^n, KU^{n+1}]$
- (9) $P::DP[KU^n, EP[KR^n, KU^{n+1}]]$

により KU^{n+1} を取り出す。

- (10) P :: 図 8 のように KU^{n+1} の一部を利用して
(例えば上位 64bit) K_D とする。
- (11) P :: EC [K_D , DATA]
- (12) P :: 再生機能のロックの解除を行う
- (13) S :: 月に一度など、3.2.4. 節の数式 1 を用いて
クリエイタの報酬額を計算する。

本方式では、視聴率の不正操作を防止するために、通信される使用記録の成りすましや、HDD 上に格納されている使用記録の改ざんを防がねばならない。よって、 KU^n の更新のたびに K_D を変更することにより、使用記録のセキュリティを高めている。

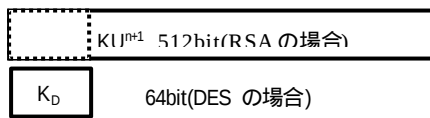


図 8 : K_D の作成

4.4. 部分集合モデルの考察

4.4.1. 要求条件からの考察

前記の要求条件を解決したか検証する

- (条件1) 会員ならば コピーフリー 使い放題とする
- (条件2) 非会員は視聴できない
- (条件3) クリエイタには視聴率に応じた報酬が分配される
上記 3 条件は、明確なので説明を略す。
- (条件4) 定額料金を払わない会員は視聴できなくなる
定額料金を払わないと、4.3.5(4)により以降に処理が進まない。よって 4.3.5.(12)が行われないので、再生機能はロックされたままになり再生は禁止される。
- (条件5) 視聴率はクリエイタによって操作できない
視聴率の操作の仕方として、使用記録の改ざん(なりすまし、連続再生、コンテンツ ID の改ざん、再生ソフトのコピー、が想定される。は、使用記録が暗号化されており、かつ暗号化鍵 K' が、定期的に変更されるため、使用記録の改ざんは困難である。は、フィルタを用いることによって防ぐことが可能である。は、4.3.1(2)より署名が施されるので、改ざんは困難である。は、やはりフィルタにより防がれる。また、全体的にいえることであるが、一部の使用記録を改ざんしたとしても、視聴率には、さほど大きな影響を与えない。

4.4.2. 課題と応用

全コンテンツを暗号化する鍵は K_s で共通あり、これを変更することはできないので、カプセルコンテンツのセキュリティレベルは、それほど高いとはいえない。しかし、部分集合モデルは、提案方式を擬似的に実現するモデルであるため、提案方式と同様、コンテンツのアクセス制限は、それほど重要ではない。むしろ、視聴率の不正操作の方が、問題であり、これについては、先に説明したように、何重かの防止策が組み込まれている。

また、この部分集合モデルは、後払い制にして使用量に応

じて課金するモデルにすると、超流通²¹にも応用できる。

5. まとめ

P2P による不正コピー問題は、解決困難であるため、現行のコンテンツ流通方式は、成立困難であることを示した。提案方式は、コピーフリー かつ使い放題なので、提案方式が実現すると、不正コピーがなくなり、クリエイタの報酬が確保される。また、段階的な導入用の部分集合モデルの方式も示した。

参考文献

- 1 藤井ほか :自由度の高い私的コピーを実現する著作権保護方式, 情報処理学会研究報告, Vol2001, No11(EIP-9), pp. 39-46(2001).
- 2 KdM コンテンツフォーラム.
- 3 日経新聞 2001.7.10.
- 4 デジタルコンテンツ白書, (財)デジタルコンテンツ協会, 2001.
- 5 Napster, <http://www.napster.com/>
- 6 Gnutella, <http://gnutella.wego.com/>
- 7 ナップスターに代わるファイル交換システム,
<http://www.hotwired.co.jp/news/news/20010910105.html>
- 8 JEXTA, <http://www.sun.com/p2p/>
- 9 日経産業新聞 2001.11. 1.
- 10 青木: デジタルコンテンツ流通の展望と今後の課題, 通信工業, 2001/2, pp.6-12.
- 11 ナップスターの利用は5月下旬以降に36%減, 他のファイル共有サービスが急進,
<http://itpro.nikkeibp.co.jp/free/ITPro/USNEWS/20010724/10>
- 12 芳尾: Napster 知らずして, NIKKEI ELECTRONICS 2000.10.9(no.780), pp125-145).
- 13 Open Platform Initiative for Multimedia Access
<http://www.opima.org/>
- 14 福田: 情報社会観を巡る対立について, 情報文化学会論文誌, Vol.7, No.1, pp.29-36(2000).
- 15 コンテンツID フォーラム, <http://www.cidf.org/>
- 16 Online Music Subscription Services Can Succeed at \$5 Per Month, But Consumer Expectations Will Not Be Met,
<http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/07-25-2001/0001541317&EDATE=>
- 17 有料音楽配信サービスの月額利用料は5ドルが妥当,
<http://biztech.nikkeibp.co.jp/wcs/show/leaf?CID=onair/biztech/inet/136186>
- 18 日経マルチメディア 1997.9
- 19 名和: 学術情報の電子化と市場化, あいみっく, 21(3) July, 2000, pp.15-21.
- 20 Merkle, R.: Secrecy, Authentication, and Public Key Systems. Ph. D. Thesis, Stanford University, June 1979.
- 21 森: デジタル革命とその未来を支える基盤技術, 情報処理学会論文誌, 2000.11.