視聴率に基づく利益分配型コンテンツ流通方式の安全性の検討

藤井 治彦† 後藤 真一郎† 新井 克也† 花木 三良† 塩野入 理‡
NTT 情報流通プラットフォーム研究所† NTT サイバーソリューション研究所‡

1．はじめに

Ｐ２Ｐ(Peer to Peer)による商用サービスを展開していくためには，Ｐ２Ｐの特徴を活用したコンテンツ流通方式が必要である．筆者らは，視聴率による利益分配型コンテンツ流通方式を考案した[1](以下，視聴率方式と呼ぶ)．本稿では，その視聴率方式の安全性を更に向上させるための検討を行う．

2．視聴率方式の概要

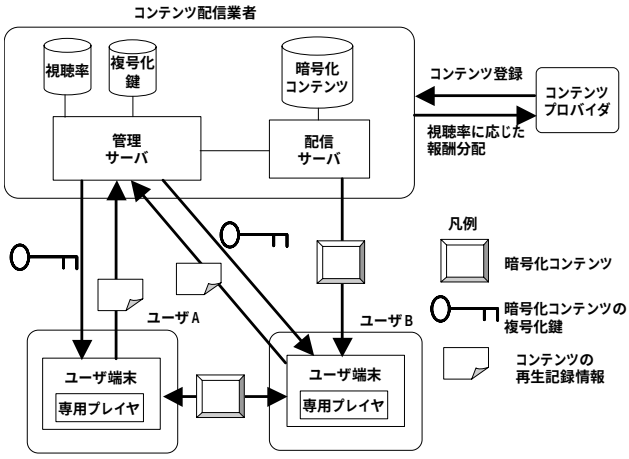

図１　視聴率方式

視聴率方式(図１)は，ユーザに対して定額料金でコンテンツを使い放題とする会員制ビジネスモデルを実現する．視聴率方式により構築されるシステムは，暗号化コンテンツを配信する配信サーバ，および暗号化コンテンツの復号鍵の配信とユーザ端末から送られるコンテンツの再生記録情報を管理する管理サーバから構成される．配信サーバから配信される暗号化コンテンツはＰ２Ｐによりユーザ同士で共有することが可能であるが，コンテンツの再生のためには管理サーバから復号鍵が配信される必要がある．復号鍵の配信時に，ユーザ端末からはコンテンツの再生記録情報が送信される．管理サーバはユーザ端末からの使用記録情報を集計し，各コンテンツの利用率（視聴率）を計算してコンテンツプロバイダに対して視聴率に応じて報酬を分配する．

A Study on Security of the Usage-based Profit-sharing Content Distribution System
Haruhiko FUJII, Shinichiro GOTO, Katsuya ARAI, Miyoshi HANAKI
NTT Information Sharing Platform Laboratories
Osamu SHIONOIRI
NTT Cyber Solutions Laboratories

3．視聴率方式の問題点

視聴率方式では，ユーザ間でコンテンツを共有しやすくするために，共通鍵暗号方式に基づいて，全てのコンテンツを同一の鍵で暗号化・複号化する．その鍵は配信されたユーザ端末内でファイルとして保存され，他のマシンに容易にコピーして使用できるため，鍵が会員以外のユーザに漏洩すると，全てのコンテンツが不正に再生されてしまうことになる．視聴率方式をＰ２Ｐ商用サービスに適用するには，①コンテンツの不正再生を極力防ぐ必要がある．一方，Ｐ２Ｐ商用サービスは②コンテンツや鍵の配信トランザクションの負荷がＰ２Ｐ商用サービスを提供するシステムに影響を与えない，③ユーザ間で簡便にコンテンツを共有できることが求められる．

安全性を向上させる手段として，鍵数を増やしなおかつ鍵自体にコピープロテクトを施すことが有効であるが，コンテンツごとに鍵を変え，その鍵をコピープロテクトする手法[2]では，鍵の配信数が非常に多くなり上記②の阻害要因になる．また，コンテンツをＰ２Ｐで共有できたとしても鍵はコピー不可能なので，管理サーバから毎回再配信せねばならず，上記①，②両方の阻害要因になる．

本検討では，上記①，②，③を満足する方式を以下に述べる．

4．コンテンツのグループ化

音楽やニュース，映画などマス向けコンテンツの一般的な特性として，時間の経過とともに商品価値が減少し，更に時間の経過とともに鍵の情報が漏洩し，不正にファイル共有される確率が高くなると本検討では仮定する．

上記仮定に基づいて本稿ではコンテンツをリリース時期ごとにグループ化し，ある期間単位で共通の鍵（以下，期間鍵と呼ぶ）を用いて暗号化することとする．ユーザ端末は，ある期間にリリースされた暗号化コンテンツに対して，端末内にその期間鍵が存在しない場合に，管理サーバに対して鍵配信要求を行う．管理サーバが

該当する期間鍵をユーザ端末に配信すると，その期間鍵はユーザ端末に保存される．これ以降同じ期間にリリースされた別の暗号化コンテンツに対して鍵配信要求を行っても，既にユーザ端末内には該当する期間鍵が存在するので，期間鍵は配信されない．図２は以上述べた鍵配信要求のアルゴリズムを示している．

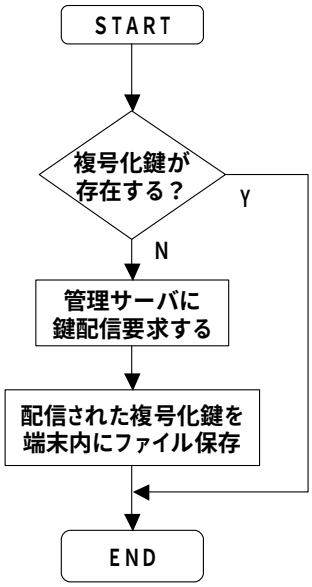

図２　鍵配信要求のアルゴリズム

表１は，各ユーザが，ある時期（９月）にどのような順番でコンテンツを再生したかを表す図である．期間鍵の期間は月単位とする．ユーザＡ，Ｂ，Ｃはそれぞれ７，８，９月にサービスに加入したものとし，Ａは既に７，８月の期間鍵を，Ｂは８月の期間鍵を所有し，Ｃはどの期間鍵も所有していないものとする．Ａ，Ｂ，Ｃは表１のコンテンツ行にあるコンテンツをそれぞれ同じように再生するものと仮定する．反転している部分は，ユーザ端末から管理サーバに対して期間鍵の要求が発生したことを表す．表中，K_{Y} 月はＹ月の期間鍵，$C_{Z}(K_{Y\,月})$はＹ月の期間鍵で暗号化されたＹ月リリースのコンテンツ（コンテンツ番号Ｚ）をそれぞれ示す．さらに表中の白抜きのセルは，期間鍵が当該日に初めて配信されたことを示す．

Ａは７，８月リリースのコンテンツの期間鍵 $K_{7\,月}$, $K_{8\,月}$を既に所有しており９／１の時点では期間鍵の要求なしに再生できる．９／２は９月リリースのコンテンツ $C_2(K_{9\,月})$の再生のために初めて期間鍵 $K_{9\,月}$の要求をしている．９／３以降の再生においては全ての月の期間鍵を持っているので期間鍵の要求を全くしていない．同様にＢは期間鍵 $K_{8\,月}$のみ所有しているので９／１と９／２に期間鍵を要求しており，Ｃは９月加入なので期間鍵を全く所有しておらず，９／１，９／２，９／４に要求を行うことになる．

仮に期間鍵が漏洩し，解読されても，当該月以外のコンテンツには影響を与えないため，被害の影響範囲は当該月のみに限定される．またコンテンツ数がどのように増加しても，ユーザの加入期間が長くなるほど期間鍵の配信は月一回に近づく．

表１　期間鍵の要求の例（９／１から）

再生日	９／１	９／２	９／３	９／４	９／５
コンテンツ	$C_1(K_{7\,月})$	$C_2(K_{9\,月})$	$C_3(K_{9\,月})$	$C_4(K_{8\,月})$	$C_5(K_{8\,月})$
Ａ	$K_{7\,月}$	$K_{9\,月}$	$K_{9\,月}$	$K_{8\,月}$	$K_{8\,月}$
Ｂ	$K_{7\,月}$	$K_{9\,月}$	$K_{9\,月}$	$K_{8\,月}$	$K_{8\,月}$
Ｃ	$K_{7\,月}$	$K_{9\,月}$	$K_{9\,月}$	$K_{8\,月}$	$K_{8\,月}$

また本検討ではユーザ登録時に，ユーザ端末を一意に識別する情報ＨＩＤ（Hardware ID:ハードディスクのボリュームナンバーなど）を管理サーバ側に送信する．管理サーバは，ユーザ端末からの期間鍵の要求があった場合には，ＨＩＤを用いて期間鍵を暗号化して送信し，ユーザ端末はＨＩＤから，暗号化された期間鍵を復号化し，復号化された期間鍵を用いて暗号化コンテンツの復号および再生を行う．復号化された期間鍵およびコンテンツはメモリ上にのみ存在し，再生が終了すると消去され，暗号化された期間鍵とコンテンツのみが残る．

以上のように本検討を視聴率方式に適用すれば簡便にユーザ間でファイル共有が可能で，かつコンテンツの不正再生を極力防ぎつつ，鍵の配信数が従来の方式[2]に比べて非常に少なく抑えられ，３章の要求条件①，②，③を満足する．

５．おわりに

本稿では，視聴率方式の安全性を向上させる手法を示した．今後，実装および試験による本検討の妥当性評価を行う予定である．

参考文献

[1]藤井他：“視聴率による利益分配型コンテンツ流通方式の提案”，情報処理学会研究報告，Vol.2001，No.118（EIP-14），pp.23-30(2001)．
[2]上野他：“不正コピー防止を考慮したコンテンツ販売システム”,情報処理学会第７回電子知的財産・社会基盤研究会 7-3,pp.17-24(2000)．